
مركز التميز لأمن المعلومات
Center of Excellence in Information Assurance







أمن المعلومات

بلغة ميسرة

تأليف

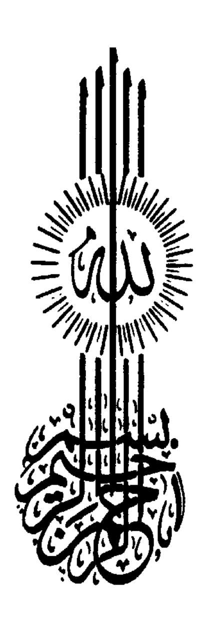
د. خالد بن سليمان الغثبر

د.مهندس/ محمد بن عبدالله القحطاني

تقديم

معالي الدكتور محمد بن إبراهيم السويل

رئيس مدينة الملك عبدالعزيز للعلوم والتقنية





المعلومات

تأليف

د. خالد بن سليمان الغثبر

CISSP, CISM, PMP,
MCSE:Security, Security+,
BS7799 Lead Auditor

د. مهندس محمد بن عبدالله القحطاني

CISSP,ISS, PMP

بلغة ميسرة

تقديم

معالي الدكتور محمد بن إبراهيم السويل

رئيس مدينة الملك عبدالعزيز للعلوم والتقنية

فهرسة مكتبة الملك فهد الوطنية أثناء النشر

القحطاني ، محمد عبدالله علي

أمن المعلومات بلغة ميسرة / محمد عبدالله علي القحطاني ؛

خالد سليمان عبدالله الغثبر – الرياض ، 1429هـ

000 ص ؛ 17 × 24سم

ردمك : 978-603-00-1325-8

1- أمن المعلومات 2- أمن الحواسيب أ. الغثبر، خالد سليمان عبدالله (مؤلف مشارك) ب. العنوان

ديوي 005,8 1429/5492

رقم الإيداع : 1429/5492

ردمك : 978-603-00-1325-8

الطبعة الأولى



1429هـ - 2009م

عن المؤلفــين

٭ د. خالد بن سليمان الغثبر

يعمل حالياً أستاذاً مساعداً في كلية علوم الحاسب و المعلومات بجامعة الملك سعود، وقد شارك في عديد من اللجان على مستوى الكلية و الجامعة والوزارة، وهو مستشار لعدة جهات حكومية وخاصة. شارك في إعداد الدراسات الأمنية وتقييمها، والإشراف عليها في عدد من الجهات المختلفة. يترأس مجموعة الاهتمام بأمن المعلومات في جمعية الحاسبات السعودية. حصل على درجة البكالوريس في نظم المعلومات من جامعة الملك سعود مع مرتبة الشرف، ثم الماجستير و الدكتوراه مع مرتبة الشرف من جامعة جورج ماسون في الولايات المتحدة الأمريكية. حصل على شهادات تخصصية عالمية في مجال أمن المعلومات وإدارة المشاريع. له العديد من المؤلفات العلمية المتخصصة في أمن المعلومات، وله مقالات أسبوعية في جريدة الاقتصادية، ويلقي عديداً من المحاضرات ويقيم الدورات التدريبية في مجال أمن المعلومات.

٭ د. مهندس محمد بن عبدالله القحطاني

حصل على بكالوريوس علوم الحاسب الآلي من جامعة الملك سعود مع مرتبة الشرف الأولى، وماجستير هندسة البرامج مع مرتبة الشرف الأولى من جامعة جورج ماسون بالولايات المتحدة، ثم دكتوراه أمن المعلومات مع مرتبة الشرف الأولى من جامعة جورج ماسون أيضاً، وقد أدار عدداً من مشروعات تقنية المعلومات تزيد قيمتها عن

750 مليون ريال، وكانت في مجال تطوير البرمجيات وبناء الشبكات وأمن المعلومات، ومتمرس في منهجية إدارة المشروعات بحسب منهج PMI. ويعمل مستشاراً لأمن المعلومات في جامعة الملك سعود، كما يعمل مستشاراً تقنياً لدى عدد من الجهات الحكومية والشركات. إضافة إلى هذا فقد أدار عدداً من الشركات ويعمل حالياً مديراً عاماً لشركة متخصصة في مجال نظام ساب (حزمة برامج متنوعة من ضمنها برامج لتخطيط موارد المنشآت ERP). له مشاركات بحثية في عدد من المحافل الدولية والمحلية. كما له عدد من الأبحاث المنشورة في محافل دولية ومحلية. وهو حاصل على عدد من الشهادات المهنية في مجال أمن المعلومات وإدارة المشروعات وكذلك هندسة البرامج

ويمكن الاتصال به على بريده الشخصي:
dr.mohammad.alkahtani@gmail.com

تقديـــم

إن التخريـب والسـرقة – بمـا فيهـا سـرقة المـال، أو المنقـولات الثمينـة، والمعلومـات المهمـة مـن الآخـرين، وإيقـاع الضـرر بهـم– مـن أقـدم الأخطـار الـتي يتعرض لها الإنسان. وتختلف دوافع التخريب والسرقة من شخص لآخر؛ ولكن في النهاية هناك طرف يقع عليه الضرر وتطاله الخسارة. ففـي الماضـي، وخصوصـاً قبل ظهور الوسائط الإلكترونية لتخزين المال والمعلومات ونقلها، كـان مـن اليسير اكتشـاف السـرقة وبسـرعة، لأن السـارق لابـد أن يـترك – في معظـم الأحـوال أثـرا لفعلتـه مثـل قفـل مكسـور، أو بـاب مهشـم ومـا شـابه ذلـك، إلا أنـه مـع ظهـور الإنترنت، واتساع نطـاق اسـتعمالاته قـد يصـعب اكتشـاف أثـر السـرقة ولـذلك لا يشعر المتضرر بفقد المعلومة أو المال إلا بعد فوات الأوان في بعض الحالات. وسوف تتفاقم هذه الأضرار مع تسارع التقدم في مجالات الاتصالات والحاسبات، وما ينتج عن ذلك من زيادة حجم المعلومات المنقولة على شبكات الاتصـالات والمعلومـات المخزونة في الحاسبات. وما هذا إلا أحد الأعـراض الـتي يعانيهـا العـالم بأسـره عنـد استحداث تقنيات جديدة، وكما هو مسلم به فإن كثيراً من التقنيات الجديدة. تولد ومعها محاسنها ومساوئها، ويترك للإنسان تغليب جانب على آخر.

إن من أصعب مهام أخصائيي أمن المعلومات هو نقل صورة كاملة وواقعية، دون مبالغة أو تهويـل أو زيـادة في تبسـيط، لمستخدمي الوسـائط الإلكترونيـة حـول الأخطار التي تتعرض لها المعلومات المخزنة إلكترونياً، أو المنقولة عبر الإنترنت من سرقة أو تغيير. ولا تزال هذه المهام صعبة، بصـرف النظـر عـن المتلقـي، سـواء كـان مستخدما مبتدئاً، أو مديراً لشركة كبرى. ومن أبرز الأخطار ما يلي:

- تغيير البرامج أو إدخال برامج جديدة مغلوطة أو مدمرة مثل الفيروسات.
- الاطلاع غير المشروع على المعلومات السرية عن طريق التنصت على شبكات الاتصالات أو الدخول غير المصرح به إلى الشبكات أو قواعد البيانات.
- الاطلاع بصفة غير مقصودة مثل الشاشات المفتوحة و الطابعات، أو حتى تجميع ما تم حذفه في سلة المهملات.
- التزوير والتزييف بإدخال معلومات مغلوطة بسوء نية، أو عن غير قصد.
- مسح المعلومات أو إخفاؤها، أو عدم إدخال المعلومات أو تغييرها سهواً أو عمداً، وكذلك تغيير كلمات السر، أو الأرقام السرية، أو مفاتيح التشفير.

وتطول هذه القائمة كلما استجد جديد، أو استحدثت أساليب خداع وتخريب و حيل مبتكرة.

وتجاوباً مع الحاجة لدرء أخطار أمن المعلومات بدأت تظهر في الآونة الأخيرة كتب ودورات ومواد دراسية ومعاهد تقدم شهادات لأخصائيي أمن المعلومات. وامتدادا لهذا التوجه فقد قام مؤلفا هذا الكتاب بجهد بارز لتعريف القارئ العربي، من قارئ عابر إلى المختص، بأخطار أمن المعلومات وأساسيات التعامل مع هذه الأخطار وتجنبها، أو التقليل من آثارها.

إن هذا الكتاب يضيف كثيراً للمكتبة العربية، ويهدف إلى نشر الوعي بأهمية أمن المعلومات بلغة مبسطة، مع تقديم الحد الأدنى من المعلومات المفيدة لكل مستخدم عن أمن المعلومات. كما يقدم الكتاب أمثلة واقعية وموثقة تعطي القارئ

تصوراً عن الموضوع بعيدا عن التهويل. كما يخاطب الكتاب شرائح مختلفة من المجتمع بسبب سعة المواضيع، وتدرج الطرح من التبسيط إلى التعمق، حتى يجد معظم القراء بغيتهم. وبهذا التوجه فإن الكتاب يتطرق إلى السهل الممتنع. فمن السهل الوعي بأخطار أمن المعلومات بعد وقوع الضرر، ولكن من الصعب توقع الأخطار واستباقها بأخذ الاحتياطات اللازمة، ثم التعامل، معها وتخفيف آثارها بعد وقوعها.

إن موضوع أمن المعلومات موضوع في غاية الأهمية، ويمس بشكل مباشر حياة كل المتعاملين مع الوسائط الإلكترونية، وينعكس على مصالحهم وسبل أدائهم أعمالهم، ولهذا فإن نشاط البحث والتطوير في مجال أمن المعلومات ينمو بشكل متزايد، وقد يفوق كثيرا من أنشطة البحث والتطوير في المجالات الأخرى في حقل تقنية المعلومات والاتصالات. وأتوقع أن يصبح هذا الموضوع فرعا مستقلا من فروع المعرفة الإنسانية، حاله في ذلك حال بعض العلوم التي تبدأ ممارسات متفرقة، ثم تأخذ شكل علم أو فرع من علم مستقل. ومقالاً على ذلك هناك علم ذو صلة بأمن المعلومات هو علم التعمية وكسر المعمي، وبدأ هذا الفرع بشكل مجموعة من الطرق والحيل وتطور مستفيدا من أسس في الرياضيات وعلم الاتصالات ليصبح علما قائما بذاته.

ختاماً أرجو أن يجد القارئ الكريم في طيات هذا الكتاب ما يحقق له الفائدة المرجوة، ويبلغ الهدف الذي يرجوه منه المؤلفان.

د. محمد بن إبراهيم السويل

معالي رئيس مدينة الملك عبدالعزيز للعلوم والتقنية

الرياض، المملكة العربية السعودية

كان يا ما كان

فيما مضى كان أبو صويلح يحفظ أوراقه المهمة ؛ مثل صك البيت ، وعقود إيجارات المحلات ، وحسابات المؤسسة ، وملفات الموظفين ، والأسهم ، في خزانة يحتفظ بمفاتيحها في جيبه, ولم يحدث يوماً ما أن أعطى هذه المفاتيح لأي أحد ، "كائنا من كان".

و قد كان أبو صويلح يدير بطريقته البدائية أعماله ، إلى أن حثه صويلح وإخوانه على استخدام الحاسوب في إدارة أعماله, وأخذوا يحدثونه عن الثمار الكثيرة التي يجنيها من يستخدم الحاسوب في بيته أو عمله ؛ و ذكروا له أن الحاسوب كالصندوق السحري الذي يفعل الأعاجيب ، فيحصي كل شاردة وواردة ، ويخزن وثائق المعلومات ، سواء منها ما كان نصاً مكتوبا ، أم وثيقة مسموعة أم مرئية. و بهذا يتمكن أبو صويلح من أن يخزن حسابات المؤسسة ، وملفات الموظفين في الحاسوب ، إضافة إلى ذلك فإنه ييسر للمرء استرجاع المعلومات متى شاء ، وعرضها بالطريقة التي يراها مناسبة. كما أنه يسهل طبعها ملونة وغير ملونة. وهذه مسألة مهمة لأبي صويلح الذي يضع ميزانية سنوية لمؤسسته ، ويحسب زكاة ماله بناء على موقفه المالي.

وقالوا له أيضاً إن الحاسوب إذا ربطته بشبكة الإنترنت أبدى لك ما كنت جاهلاً ، وجاءك بأخبار القاصي والداني, فكان كما يقول طرفة بن العبد في معلقته :

ستبدي لك الأيام ما كنت جاهلاً

ويأتيك بالأخبار من لم تُزود

بل فاق وصف طرفة ذلك أنه يبدي لك في لحظات ما كان يُعلَم في أيام ، وهذه الخاصية أعجبت أبا صويلح كثيراً ، لأنها تمكنه من معرفة أخبار أسعار الأسهم دون

الحاجة للاتصال بأصحابه من تجار الأسهم، أو الذهاب إلى قاعات تداول الأسهم في البنك، بل يمكنه كذلك متابعة أعمال مؤسسته وهو في بيته، أو في أي مكان آخر.

ولكن أبا صويلح رجل حنكته السنون، وعلمته أن "لا يدخل رأسه إلا فيما فيه خلاصه، " فأخذ يسأل المتخصصين في مجال الحاسوب عن ذلك الصندوق السحري ما له وما عليه. وضرره ونفعه، فبين له المتخصصون أن للحاسب مزايا تعين مستخدمه على إدارة أعماله، سواء كانت على مستوى الفرد أو المؤسسة، وأكدوا له أنه قريبا سيأتي اليوم الذي سيتغير فيه معنى كلمة "أميّ" التي تطلق اليوم على من لا يجيد القراءة والكتابة، وستطلق بدلا من ذلك على من لا يجيد استخدام الحاسب.

غير أنهم حذروه من أن هناك فروقا جوهرية بين الأخطار التي تتعرض لها المعلومات المخزنة في أجهزة الحاسوب، وتلك التي تتعرض لها المعلومات المكتوبة "على ورق". وملخص ما قالوه هو:

(1) أنه فيما مضى كانت المعلومات تخزن على أوراق، وهذه يمكن حيازتها في موضع واحد، وحمايتها ومنع وصول الآخرين إليها بوضعها في مكان آمن كالخزانة، أو غيرها من وسائل الحفظ، كما يمكن وضع حرس حول مكان تخزينها، ولذلك فإن من أراد سرقتها لن يجد بدا من اختراق إجراءات الحماية هذه، وفي هذا مشقة ومخاطرة. أما من أراد سرقة معلومات مخزنة في الحاسوب فإنه في أغلب الأحيان لا يكون مضطرا لمغادرة مكانه، بل يمكنه التسلل عبر "الأسلاك" التي تربط "الكمبيوترات" بعضها ببعض، وسرقة المعلومات دون أن يراه أحد.

(2) إن نسخ الوثائق التي فيها المعلومات يحتاج إلى آلات تصوير أو كاميرات، لكن نسخ الوثائق المخزنة في الحاسبات لا يتطلب أيا من هذا.

(3) إن الأخطار التي تتعرض لها المعلومات يمكن تقسيمها إلى ثلاثة أصناف:

(أ) **خطر كشف المعلومات السرية**: السطو على المعلومات قد ينتج عنه اطلاع المهاجم على معلومات ما كان ينبغي له الاطلاع عليها، وهذا يكشف معلومات كان مالكوها يرغبون في حفظها سرية، وهذا الصنف يقع على المعلومات المخزنة على أوراق، كما يقع على تلك المخزنة في الحواسيب على حد سواء.

(ب) خطر حرمان مالك المعلومات من الوصول إليها عند الحاجة: إن السطو على المعلومات المخزنة على الورق قد ينجم عنه حرمان صاحب المعلومات منها إذا كانت النسخة المسروقة هي النسخة الوحيدة. كما أن هذا النوع من الأخطار يمكن أن يحيق بالمعلومات المخزنة في أجهزة الحاسوب.

(جـ) **خطر تغيير المعلومات**: المعلومات المخزنة على أوراق تتمتع بخاصية مهمة هي أن أي تغيير عليها يسهل للإنسان - في أغلب الأحيان- ملاحظته، ولذلك فإنه يصعب على من يسطو أن يغير تلك البيانات دون ترك آثار تدل على ذلك. أما البيانات المخزنة على وسائط مغناطيسية، فإن العبث بها دون ترك آثار تدل على وقوع ذلك يعد أمراً ميسوراً، ولذا يلزم اتخاذ إجراءات حماية خاصة للحيلولة دون ذلك.

(4) أن تداول الوثائق الورقية المسروقة ونقلها ونشرها يتطلب جهداً ووقتا وكلفة تتجاوز ما هو مطلوب في حال تخزينها في الحواسيب.

(5) إن يسهل على مالك المعلومات المهمة أو السرية التخلص من الأوراق التي بها تلك المعلومات، وذلك بفرمها، أو حرقها، أو غير ذلك من الوسائل المعروفة. أما الطريقة المعتادة لحذف الملفات التي تحتوي على المعلومات المخزنة في الحواسيب، فحتى مع سهولتها و يسرها، فإنها - في حقيقة الأمر- لا تتخلص من تلك الملفات وإنما تخفيها عن عين مستخدم الحاسوب، و يمكن - في أغلب الأحيان- استرجاعها، وهذا الأمر يعطي شعوراً زائفاً بأنها لم تعد في متناول لصوص المعلومات.

ولما تبين لأبي صويلح أنه لا يمكنه أن يغلق على ذلك الجهاز في "التجوري" وقع الخبر عليه كالصاعقة, وزاد المصاب وعظم الخطب لما علم أنه تخرج من جهازه أسلاك لو ربطت بجهاز آخر أصبح غيره قادرا على رؤية المعلومات المخزنة في جهازه. لكنهم أخبروه بأن جهازه يربط بأجهزة أخرى توفيراً للمال. فبدلاً من أن يكون عند كل موظف جهاز حاسوب وطابعة وماسحة ضوئية يمكن أن تربط الأجهزة بشبكة واحدة، ويكتفى بطابعة واحدة وماسحة ضوئية يستخدمها جميع العاملين بمؤسسة أبي صويلح، و يمكن أن توضع الطابعة أو الماسحة في مكتب أحد الموظفين الذين هم في موضع الثقة من أبي صويلح، بل يمكن أن توضع في مكتب أبي صويلح نفسه.

ولم تنته مشكلات أبي صويلح مع الحاسوب بعد؛ فلقد سمع جاره أبا حمد يذكر أن هناك أناسا يسمون "الهاكرز" "يدخلون" من أجهزتهم بطريقة سحرية على مواقع الشركات و"كمبيوترات الناس"، فيعيثون فيها فسادا، و يسرقون المعلومات التي فيها، وأن هناك جراثيم أو فيروسات تنتشر بطريقة غريبة فتصيب أجهزة الحاسوب فتدمر ما فيها من معلومات، وأحيانا تتلف الجهاز نفسه. وتعجب أبوصويلح من أولئك الذين يربطون حاسباتهم بشبكة الإنترنت، إذا كانت كل هذه الشرور تأتي منها، فأخبر أن شبكة الإنترنت في حقيقتها ظاهرة تقنية عميقة الأثر غيرت كثيراً من الأشياء في حياتنا، و ساهمت في تسهيل كثير من الأعمال، وخفض النفقات، وتيسير الوصول إلى المعلومات، كما أنها البوابة التي دخلت معها كثير من التطبيقات المفيدة للأفراد؛ والشركات والمؤسسات. فيمكن لشركة ما أن تضع معلومات عن الخدمات التي تقدمها في موقعها على شبكة الإنترنت، ويمكنها كذلك طلب عروض التوريد أو التنفيذ أو تقديمها عن طريق الإنترنت. وتجلى لأبي صويلح أنه قد غدا ضرورياً لمثله من رجال الأعمال وكذلك المدراء في الهيئات الحكومية وغير الحكومية، تحصيل قدر كاف

من المعرفة عن الإنترنت، والتقنيات المرتبطة بها، خصوصا بعد أن تبين له أن هذه الشبكة تشهد نموا لا مثيل له، سواء في المستوى الأفقي أم الرأسي، فنموها الأفقي يتمثل في زيادة عدد الأجهزة المرتبطة بشبكة الإنترنت بشكل متنامٍ. أما النمو الرأسي فالمقصود به زيادة عدد التطبيقات التجارية وغير التجارية التي تستخدم شبكة الإنترنت. ومما يدعم هذا النمو توجه كثير من الدول، بما فيها المملكة العربية السعودية، لتطبيق الحكومة الإلكترونية، مما يؤثر كثيراً في الطريقة التي تدار بها الأعمال في القطاعين الخاص، والحكومي، وهذا بلا شك يؤثر في حياة الأفراد، طريقة عمل المؤسسات، فيتمكن الفرد، مثلاً من تعبئة المعلومات المطلوبة للحصول على جواز سفر عن طريق زيارة موقع الجهة المسؤولة عن إصدار الجوازات، ثم يذهب للحصول على جوازه، كما يمكنه تسديد فواتير الماء والكهرباء والهاتف وغيرها إذا كان جهازه مرتبطا بشبكة الإنترنت، وهذا يوفر وقته قطعا.

كما أن الشبكة أضحت وسيلة للتجارة الإلكترونية (e-commerce)، خاصة في الدول المتقدمة، وهذا النوع من التجارة جاء ليبقى، بل سيصبح الميدان الأكبر للتنافس بين الشركات في المستقبل القريب. وأهم ما يميز التجارة الإلكترونية أنها ألغت الحدود الجغرافية، فأصبح التاجر ورجل الأعمال المحلي عرضة للمنافسة من قبل شركات وأفراد خارج المدينة؛ بل الدولة التي يعيش فيها.

وفوائد استخدام الإنترنت ليست مقصورة على الشركات والمؤسسات؛ بل يستفيد منها الأفراد كذلك. فالإنسان الراغب في السفر- على سبيل المثال- يستطيع مقارنة أسعار الفنادق، وشركات الطيران، وتأجير السيارات، وعمل الحجوزات باستخدام شبكة الإنترنت، دون أن يغادر منزله أو مكتبه.

إلا أن الإنترنت سيف ذو حدين: فهي وإن كانت مصدراً للخدمات

والتسهيلات التي سبق الحديث عنها, فهي كذلك معبر لكثير من الشرور، وسبب ذلك أن الإنترنت يمكن أن تكون سلاحاً مدمراً بأيدي الأشرار الذين لديهم من المعرفة التقنية ما يمكنهم من تطوير الإنترنت لتحقيق مآربهم. كما أن فيها مواقع سيئة لا يليق بالعاقل العفيف ارتيادها، وأخرى تبث أفكارا تتناقض مع معتقداتنا. وهناك وسائل يمكن لرب الأسرة أو رب العمل استخدامها لحماية أسرته، أو مؤسسته من هذه الشرور. فمن ذلك تثبيت جدران الحماية (Firewalls)، وأنظمة كشف الاختراق (Intrusion Detection Systems) وغيرها.

ولمساعدة أبي صويلح وأمثاله في كيفية الاستفادة من خدمات الحاسوب، وشبكة الإنترنت، مع توفير الحماية اللازمة للمعلومات الشخصية والوثائق الحساسة، يأتي هذا الكتاب دليلاً للفرد ورب الأسرة، ورجل الأعمال، ومدير المنشأة، سواء كانت حكومية أم لم تكن، ويتحدث الكتاب عن بعض المبادئ المتعلقة بأمن المعلومات، ويركز على أشهر الطرق التي يسلكها الأشرار لاختراق شبكة الإنترنت، ومعدات الحاسوب، وما يقوم عليها من أنظمة معلومات، ثم يقدم الكتاب إجراءات الحماية حسب الإمكانات المتاحة. وكل هذا يعرض دون تفصيل ممل و لا إيجاز مخل.

مقدمـــة

برزت في القرن المنصرم ظواهر تقنية عديدة تركت أثراً بيناً في حياة الناس, لكن يبقى الحاسوب أبرز هذه الظواهر قاطبة، وذلك لسرعة تطوره وانتشاره، ولعمق أثره في حياة الناس، بل وفي التقنيات التي سبقته وجوداً أو لحقته، فقلما تجد آلة، أو جهازاً إلا والحاسوب جزء أصيل منه.

وقد ساهم الحاسوب في رفع نوعية الحياة التي يعيشها الناس بتذليله كثيراً من الصعوبات واختصاره للوقت والجهد، وأصبحت كثير من الأمور لا يمكن أن تسير إلا بمساعدة الحاسوب، ومن ذلك على سبيل المثال المعاملات المالية، وتنظيم رحلات الطائرات، وتشغيل كثير من الأجهزة الطبية والصناعية، إلى غير ذلك من الأمثلة التي جعلت الحاسوب ملء السمع والبصر.

ثم جاءت الإنترنت فوسمت بميسمها وجه الحياة في السنوات العشر الماضية، كما زادت مقدار الخدمات التي يُقدمها الحاسوب، فضاعفت انتشار الحاسوب وعمقت أثره ، وأحدثت ثورة في مجال المعلومات -صناعةً وحفظاً، ونقلاً ونشراً-.

[1] لمحة عن شبكة الإنترنت

إذا كان معظم الناس يملكون قدراً لا بأس به من المعرفة فيما يتعلق بالحاسوب كجهاز، فإنهم قد لا يملكون القدر نفسه عندما يتعلق الأمر بالإنترنت. وللتوضيح نقول: إن الإنترنت شبكة مكونة من شبكات , وكل من هذه الشبكات قد يحوي بدوره شبكات أصغر، وهلم جرا، حتى نصل إلى أصغر مستوى من هذه الشبكات التي تتكون من عدد من الحواسيب المرتبطة بعضها ببعض.

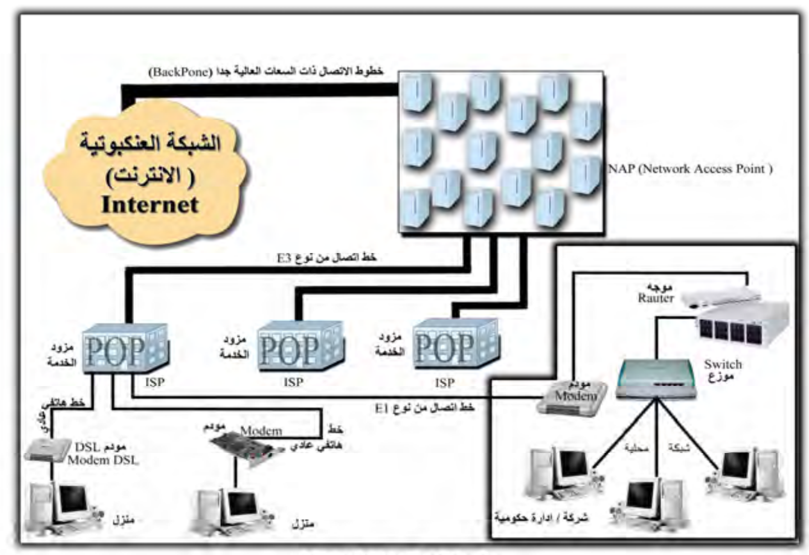
وحرص الناس على الاتصال بشبكة الإنترنت له ما يبرره، نظرا لما تقدمه من خدمات على المستوى الشخصي، والتجاري، والحكومي، فأنت إذا رغبت أن تشرح

لابنك درساً في مادة العلوم يتحدث عن محرك الاحتراق الداخلي، فإن بإمكانك أن تزور موقعاً مثل http://www.hostuffwork.com لتجد فيه شرحاً مفصلاً مدعوماً بالرسومات التوضيحية المتحركة. ومن جهة أخرى يمكن لشركة ما أن تعرض منتجاتها وتبيعها عن طريق شبكة الإنترنت، فتصل بذلك إلى عدد كبير من الزبائن. وقد اتجهت كثير من الحكومات إلى تقديم خدماتها للجمهور عن طريق شبكة الإنترنت. فإدارة المرور، مثلاً، تجعل لها موقعاً على الشبكة، وإذا كنت بحاجة إلى تسديد مخالفة فما عليك إلا زيارة الموقع ودفع الرسوم، دون الحاجة إلى الذهاب شخصياً إلى إدارة المرور.

وخلاصة القول إن المقام سيطول بنا لو حاولنا سرد الخدمات التي توفرها الإنترنت، وستكون معرفة الاستفادة منها عاملاً مهماً في نجاح الفرد والشركة والمجتمع، خاصة في زمن العولمة الذي ألغى الحدود الجغرافية تقريبا.

[2] طرق الاتصال بشبكة الإنترنت

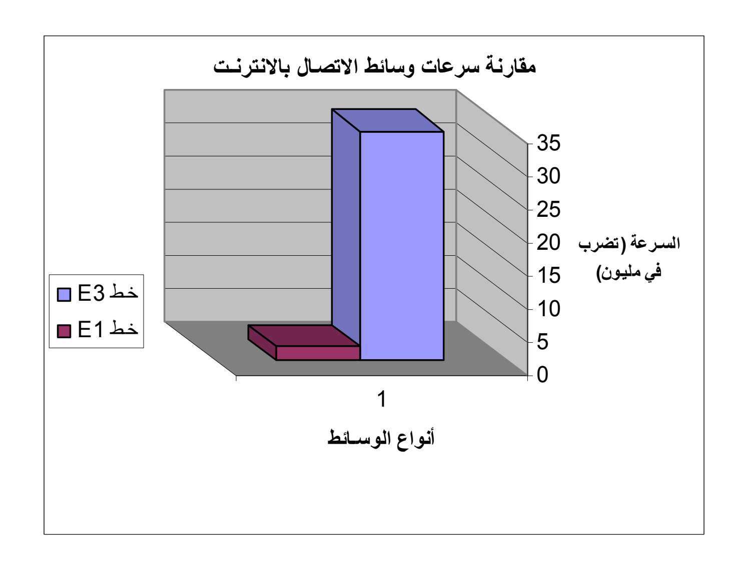
الشكل(1). هذا والربط إما أن يكون باستخدام جهاز مودم وخط هاتفي، وهذا النوع أقل أنواع الاتصال كلفة، لكنه أبطؤها، فقط تصل سرعته إلى (56 ألف نبضة في الثانية) كحد أقصى، وإما أن يكون باستخدام تقنية (DSL) التي تستخدم فيها أجهزة خاصة تسمى (DSL Modem) عندها القدرة على نقل البيانات بسرعات عالية (تتراوح بين 64 ألفاً إلى 52 مليون نبضة في الثانية)، على خطوط الهاتف نفسها، وفي كلتا الطريقتين يكون مزود الخدمة بوابتك التي تلج منها إلى عالم الإنترنت.



طرق للاتصال بشبكة الانترنت

الشكل(1): طرق الاتصال بشبكة الإنترنت.

أما الشركات، والدوائر الحكومية فإنها غالباً ما تمتلك شبكات داخلية ترتبط بمزود الخدمة بواسطة خطوط اتصال خاصة تتميز بسرعة نقل كبيرة . ومن أمثلة هذه الخطوط ما يعرف باسم (E1) الذي يعطي سرعة تصل إلى (2 مليون نبضة في الثانية)، و(E3) الذي يعطي سرعة تصل إلى (34,4 مليون نبضة في الثانية) كما في الشكل(2)، وهذه الخطوط السريعة تتصل بمزود الخدمة الذي يصلها بدوره بشبكة الإنترنت.



الشكل (2): مقارنة بين سرعة نقل المعلومات باستخدام خط E1 و E3 .

[3] الجرائم المتعلقة بالمعلومات

وكما أدخل الحاسوب والإنترنت خدمات وتسهيلات ومعارف، بل ومصطلحات جديدة فقد أعطيا عالم الجريمة أبعادا جديدة. فصار من الممكن ارتكاب جريمة اختلاس أو سرقة، أو تزوير عن بعد، وأصبحت وسائل الأمن والحماية المحسوسة من حراسات وصناديق حفظ وأماكن تخزين لا تكفي وحدها لحماية المعلومات من اللصوص. وظهر مصطلح (Cybercrime) الذي يعني الجرائم التي ترتكب باستخدام الحاسوب وشبكة الإنترنت. وقد وصل الأمر إلى أن الحكومة الأمريكية أطلقت في فبراير 2003م مبادرة لحماية المجال المعلوماتي (Cyberspace)

القــومي الأمــريكي أسمتهــا (National Strategy to Secure Cyberspace)[1]. و قــد حـذا عدد مــن الدول حذوها. ومما ينبغي ذكره في هذا المقام أن من المشروعات المقترحة في الخطة الوطنية لتقنية المعلومات في المملكة العربية السعودية مشروع إنشاء مركز وطني لأمن المعلومات، ومشروع إنشاء وحدة خاصة للمتابعة والتحقيق في المخالفات المتعلقة بأمن المعلومات[2].

ولإعطاء القارئ الكريم نبذة عن أشكال الجرائم التي يمكن ارتكابها في عالم المعلومات نسوق القصص الحقيقية التالية:

* اخترق شاب روسي شبكة شــركة (CD Universe) في عــام 1999م، وسرق منــها معلومــات 300.000 بطاقة ائتمــان تخص زبـائن الشـركة، وطلـب فدية قـدرها 100.000 دولار. ولما تلكأت الشركة عن الدفع قام بنشر المعلومات عن هـذه البطاقات على شبكة الإنترنت[3].

* في أغسطس من عــام 2002 م اكتشفـــت شـــركة (Daewoo Securities) أن ما قيمته 21.7 مليون دولاراً من الأسهم التي تديرها قد بيعت بصورة غير قانونية، وذلك بعد أن اختُرقت شبكة الحاسوب فيها[4].

---

(1) http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf

(2) مسودة الخطة الوطنية لتقنية المعلومات للخمس سنوات الأولى التي أعدتها جمعية الحواسيب السعودية عام 1424هـ.

(3) كتـــاب: (All– in–one CISSP Certification) تـــأليــف: Shon Harris و نشــــــر: MC Graw Hill.

(4) المرجع السابق.

* قام موظف إحدى الشركات الروسية في ديسمبر 2003م باختراق نظام معلومات الشركة، ورفع راتبه الشهري، ورواتب بعض زملائه، ملحقاً خسائر مالية بالشركة(1).

* في أوائل عام 2004م تلقى أحد الأمريكيين رسالة بالبريد الإلكتروني من جهة انتحلت شخصية إحدى الإدارات الفرعية في (eBay's PayPal) وهي شركة مشهورة في سوق الإنترنت، وهذه الإدارة تقدم للمشتركين فيها خدمة سداد فواتير المشتريات عن طريق الإنترنت، ولكي تقوم بذلك تحتفظ بمعلومات معينة عن هؤلاء المشتركين. وفي تلك الرسالة طلب المنتحل من الشخص المستهدف أن يحدث بياناته الشخصية و إلا تعرض حسابه لديهم للتوقيف المؤقت، ولأجل تحديث بياناته أعطي رابطا (Link). و لما قام المستهدف بالنقر على الرابط لتحديث بياناته أخذه الرابط إلى موقع يشبه موقع (eBay's PayPal)، فأدخل بياناته الشخصية التي منها اسمه الكامل ورقم بطاقته الائتمانية ورقم بطاقته السري، ورقم حسابه في البنك، ورقم هويته وتاريخ ميلاده ..إلخ. والحقيقة أن ذلك الموقع لم يكن سوى غطاء لاستدراج الضحية لتقديم معلومات مهمة استخدمها الذين صمموا الموقع لشراء بضائع بقيمة 1200دولار من حساب ذلك المسكين. ولما تنبه لذلك قام بإشعار البنك لإيقاف العمل ببطاقته الائتمانية، وظن أن الأمر قد انتهى عند ذلك الحد، وما راعه إلا أن جاءته رسالة بعد أشهر قليلة من شركة تأمين السيارات التي يتعامل معها تشرح فيها الشركة سبب رفضها طلبه قرضا قدره 30,000 دولار. وحقيقة الأمر أنه لم يطلب ذلك القرض بل طلبه أولئك الذين سرقوا معلوماته الشخصية عن طريق الإنترنت(2).

---

(1) http://www.crime-research.org/news/17.12.2004/852/.

(2) http://www.crime-research.org/articles/806/.

[4] مكونات أمن المعلومات

عند ذكر كلمة أمن المعلومات، وجرائم الحاسوب فإن ما يتبادر إلى الذهن غالباً هو كشف معلومات كان يجب أن تبقى سراً ؛ والحقيقة أن الحفاظ على سرية المعلومات لا يعدو أن يكون جانبا واحداً من جوانب الأمن ؛ أما المتخصصون فيرون لأمن الحاسوب والمعلومات مكونات ثلاثة على درجة واحدة من الأهمية ؛ وهذه المكونات هي :

(أ) سـرية المعلـومات (Data Confidentiality): وهذا الجانب يشمل كل التدابير اللازمة لمنع اطلاع غير المصرح لهم على المعلومات الحساسة أو السرية. وهذا، كما أسلفنا، هو ما يتبادر إلى ذهن السامع عند الحديث عن أمن المعلومات، ومن أمثلة المعلومات. التي يُحرص على سريتها : المعلومات الشخصية، والموقف المالي لشركة ما قبل إعلانه، والمعلومات العسكرية.

(ب) سلامـة المعلومـات (Data Integrity): خلافاً لما جاء في الفقرة السابقة، فإنه لا يعنينا هنا أن نحافظ على سرية المعلومات، ولكن ما يهمنا هنا هو اتخاذ التدابير اللازمة لحماية المعلومات من التغيير . وهناك أمثلة كثيرة لهذا المطلب. فقد تنشر جهة ما قوائم أسماء المقبولين ممن تقدموا بطلبات للعمل لديها، وكما نرى جميعاً فإننا عندما نتحدث عن أمن هذه القوائم نعني حمايتها من التغيير، فمن المحتمل أن يقوم شخص ما بحذف بعض الأسماء، وإدراج أسماء أخرى بدلاً منها، مسبباً كثيراً من الإرباك للناس والحرج للجهة المعنية. أو ممكن تغيير مبلغ التحويل من 100 ريال إلى 1000000 ريال.

(جـ) ضمان الوصول إلى المعلومات والموارد الحاسـوبية (Availability): إن الحفاظ على سرية المعلومات وسلامتها أمر مهم و لا ريب، لكن هذه المعلومات تصبح غير ذات قيمة إذا كان من يحق له الاطلاع عليها لا يمكنه الوصول إليها، أو أن

الوصول إليها يحتاج وقت طويلاً. ويتخذ المهاجمون وسائل شتى لحرمان المستفيدين من الوصول إلى المعلومات، ومن هذه الوسائل حذف المعلومات نفسها أو مهاجمة الأجهزة التي تخزن المعلومات فيها وشلها عن العمل.

[5] العناصر الضرورية لشن الهجمات الإلكترونية

قبل الاسترسال في الحديث علينا أن ندرك أن شن الهجمات الإلكترونية على أنظمة المعلومات، - أو بعبارة أدق على المعلومات أو الأنظمة الحاسوبية والشبكات التي تخزن فيها المعلومات وتنتقل عبرها- له ثلاثة عناصر[1]:

(أ) وجود الدافع: إن من يهاجم نظام معلومات ما لابد أن يكون هناك ما يدفعه لذلك. فقد يكون الدافع هو الحصول على المال، وقد يكون الدافع هو الرغبة في الانتقام من الجهة المستهدفة، أو الرغبة في الاستئثار بأكثر قدر من الزبائن، كما هو الحال بين الشركات المتنافسة. فقد تطلب شركة ما من أحد المحترفين في مهاجمة أنظمة المعلومات اختراق الموقع التابع لشركة منافسة أو تعطيله على الشبكة العنكبوتية؛ لمنع وصول الزبائن لموقع الشركة المستهدفة. وأحياناً يكون الدافع رغبة المهاجم في إثبات قدراته الفنية، وقد يهاجم المهاجم لأغراض سياسية كما حدث لموقع قناة الجزيزة في 27 مارس 2003م، والذي يبدو أن الدافع هو وراء الهجوم كان هو اعتقاد المهاجمين أن قناة الجزيزة كانت منحازة للجانب العراقي إبان الغزو الأمريكي للعراق. ونتج عن هذا الهجوم أن مرتادي القسم الإنجليزي من الموقع كانوا يشاهدون صورة تمثل العلم الأمريكي مكتوباً تحتها ما معناه: "دعوا الحرية تدق - ناقوسها" كما في الشكل(3) - في إشارة إلى أن أمريكا إنما جاءت لتحرير العراقيين. أما مرتادو القسم

---

(1) دورة: "Hacking Exposed" التي عقدها: "Irvin Rankin" من شركة: "Symantics" في الفترة من 9- 13 مارس 2004م بمدينة الرياض.

العربي من الموقع فقد كانوا يوجهون إلى موقع إباحي.



الشكل(3): الصورة التي كانت تظهر في موقع قناة الجزيرة أثناء تعرضه للهجوم.

(ب) وجود طريقة لتنفيذ الهجوم: من البديهي أن المهاجم لن يتمكن من شن هجوم ناجح ما لم يكن لدية تصور وخطة واضحة لطريقة هجوم تحقق الغرض، وهذا هو الفارق بين المهاجمين المحترفين وغير المحترفين. ولصد هذه الهجمات أو تخفيف أضرارها يجب علينا معرفة طرق الهجوم وخططه، ومتطلبات نجاح التنفيذ.

(جـ) وجود الثغرات: الثغرة (Vulnerability) في هذا السياق مصطلح يقصد به وجود نقطة ضعف في تصميم (Design) أو تهيئة (Configuration) البرمجيات، أو قواعد تخزين المعلومات، أو الأجهزة التي تحفظ فيها المعلومات، أو معدات أو برامج تشغيل الشبكات التي تمر المعلومات خلالها. ونقاط الضعف هذه هي الثغرات التي يتسلل المهاجم من خلالها لإحداث الدمار الذي يريده. وإذا كنا نسعى لحماية أنظمة معلوماتنا فعلينا فحص شبكاتنا ومعداتنا وبرمجياتنا لتحديد نقاط الضعف الموجودة وكيفية معالجتها. والذي يحدث غالباً أنه عندما يكتشف باحث ما من خارج الشركة المصنعة لمنتج ما نقطة ضعف في ذلك المنتج -ولنضرب لذلك مثلاً نظام

التشغيل وندوز – فإن نقطة الضعف هذه تعلن في المجلات المتخصصة، أو مواقع معينة في الإنترنت. عندها تسعى الشركة المصنعة جاهدة لإنتاج علاج لنقطة الضعف المكتشفة لقطع الطريق على أي مهاجم قد يحاول استغلال هذه الثغرة. وفي مثالنا هذا تصدر شركة مايكروسوفت بريمجاً علاجياً (Software Fix) ينزله المستخدمون من مواقع الشركة لتحديث أنظمة التشغيل لديهم.

كما أسلفنا قد يحاول بعض المهاجمين استغلال نقطة الضعف المكتشفة لشن هجمات، كأن يطوروا برامج خبيثة تخترق نظام تشغيل ويندوز الذي لم يُحدَث باستخدام البريمج الوقائي الذي أصدرته الشركة المصنعة. ومن أمثلة هذه الثغرات ما جاء في أنباء يوم 2004/12/17م من أن هناك ثغرة في نظام إكسبلورر (أحد منتجات شركة مايكروسوفت) الذي يُستخدم لتصفح المواقع على شبكة الإنترنت. ولو افترضنا أن رب أسرة يريد شراء كتب من موقع أحد المكتبات على شبكة الإنترنت، فإنه عادة يدخل اسم الموقع في الخانة الموجودة في أعلى المتصفح فيأخذه المتصفح إلى ذلك الموقع. ولكن هذه الثغرة إذا استغلت تمكن المهاجم من أخذ رب الأسرة إلى موقع المكتبة، ولكن المعروض أمامه تكون معلومات مأخوذة من موقع آخر حسب ما يحدده المهاجم.

وهناك حالات تكتشف الثغرات من قبل العاملين في الشركة المصنعة، وهنا غالبا ما تطور الشركة بريمجا علاجيا ثم تحمله في مواقع الشركة، يتلو ذلك الإعلان عن وجود الثغرة، وحث المستخدمين على تحميل البريمج الوقائي من مواقع الشركة. وفي أحيان أخرى يكون للمهاجمين قصب السبق في اكتشاف وجود الثغرات، فالمتوقع في هذه الأحوال ألا تعُرف الثغرة إلا بعد أن ينفذ المهاجم من خلالها ويكتشف حدوث الاختراق.

[6] مصادر الإخلال بأمن المعلومات

إن المعلومات أو الأنظمة التي يحتفظ بها تكون عرضة للهجوم من جبهتين مختلفتين: الجبهة الداخلية والجبهة الخارجية، ولشدة خطر الأولى فإننا سنناقشها أولاً.

(أ) المهاجمون من الداخل

لعله من المناسب أن نحدد ما نعني بالمهاجمين من الداخل، إنهم أولئك الأفراد الذين ينتمون للجهة المستهدفة، غير أنهم يقومون بأعمال تصادم جهود الجهة الرامية إلى حماية أنظمة المعلومات التي تستخدمها تلك الجهة. والمهاجمون من الداخل كانوا دوماً الخطر الذي تواجهه أي جهة، مهما كانت، سواء كانت تلك الجهة شركة أو منظمة أو حتى دولة. ولقد فاقم اختراع الحاسوب والتقنيات التي ظهرت إلى الوجود بعد ذلك الخطر الناجم عن الهجمات التي قد يشنها العدو الداخلي ضد الجهة التي ينتمي إليها ظاهراً. ويُظهر تقرير صدر في الولايات المتحدة الأمريكية عام 2003م أن 36٪ من الجهات التي شملتها دراسة مسحية أجراها مكتب التحقيق الفيدرالي (FBI) مشاركة مع معهد أمن الحاسوب (Computer Security Institute)، أو ما يعرف اختصارا باسم (CSI)، يعتبر المستخدمين من داخل تلك الجهات خطراً حقيقياً على أنظمة المعلومات التي تستخدمها تلك الجهات[1].

وسبق لوزارة الدفاع الأمريكية إصدار تقرير في عام 2000م ذكرت فيه أن 87٪ من الهجمات المكتشفة التي شنت على أنظمة المعلومات بالوزارة قام بها أشخاص من داخل الوزارة نفسها[2].

---

(1) تقرير بعنوان: "*The 2003 CSI/FBI Report on Computer Crime and Security*"، في الموقع: http://www.visionael.com/products/security_audit/FBI_CSI_2003.pdf

(2) تقرير بعنوان: "*DoD Insider Threat Mitigation*, Final Report of the Insider Threat Integrated Process Team" في 24 أبريل 2000م، في الموقع: http://www.defenselink.mil/nii/org/sio/iptreport4_26dbl.doc

ولكن بسبب الضجة الإعلامية التي تثار عادة عندما يكون الهجوم على جهة ما قادماً من خارجها مثل الإنترنت، فإن الشركات والدوائر الحكومية تولي جل اهتمامها لتحصين أنظمة معلوماتها ضد الهجمات القادمة من الخارج، وغالباً ما يكون هذا على حساب الاستعداد لصد الخطر القادم من الداخل الذي يحدث غالباً دمارا باهظ التكاليف. وبحسب تقديرات معهد أمن الحاسوب (CSI) ، فإن معدل تكاليف الهجوم القادم من الداخل هو 2.7 مليون دولار للهجوم الواحد ، بينما لا يزيد معدل الهجوم الواحد القادم من الخارج عن 57 ألف دولارا[1].

(1) **دوافع الهجوم من الداخل**: هناك أسباب عديدة قد تدفع الإنسان لشن هجوم ضد أنظمة معلومات الجهة التي يعمل فيها، ومن أهم هذه الأسباب ما يلي[2]:

(أ) **عدم الرضا**: أياً كانت مسببات عدم الرضا هذا، إلا أن الواقع يشهد أن التقنية الحديثة جعلت من مهاجمة نظم المعلومات أمراً يُشعر بالانتقام للذات، ويبعث البهجة في نفس الشخص الذي نفذ الهجوم.

(ب) **إثبات الشخص مهاراته الفنية وقدراته على تنفيذ هجوم إلكتروني**: هناك طائفة عريضة من الناس يداخلهم الشعور بالفخر إذا تمكنوا من اختراق مواقع على شبكة الإنترنت، أو وصلوا إلى قواعد بيانات محمية، ويجدون في ذلك أمراً يباهون به أقرانهم. والحقيقة أن كثيرا من هؤلاء قد لا يملكون المعرفة الحقيقية لشن الهجمات الإلكترونية، ولكن هناك مواقع على شبكة الإنترنت

(1) "Internal Threat – Risks and Countermeasures" في 2001/12/15م ، في الموقع:
http://www.sans.org/rr/papers/60/475.pdf

(2) المصدر السابق.

توفر برامج يمكن استخدامها في مهاجمة أنظمة المعلومات، ولا يتطلب استعمالها كبير معرفة بالحاسوب أو الشبكات. ولذلك كثيراً ما تسمع أشخاصاً يتظاهرون بأنهم من قراصنة الإنترنت، أو ما يطلق عليهم اسم (Hackers)، وهم في الحقيقة مجرد مبتدئين توفرت لهم برامج تعينهم على شن هجمات ما كان لهم أن يشنوها لو لا توفر هذه البرامج. ويسمي المتخصصون في مجال أمن المعلومات هذا الصنف من المهاجمين أطفال البرامج الجاهزة (Script Kiddies).

(جـ) **تحقيق المكاسب المالية**: قد يهاجم شخص ما أنظمة معلومات الجهة التي يعمل فيها لسرقة معلومات سرية يستخدمها لاحقاً لابتزاز الجهة لدفع فدية مالية.

(**2**) **حجم التهديد الداخلي**: إن الهجوم من الداخل يمكن أن يخل بأي من مكونات أمن المعلومات التي تحدثنا عنها سابقاً، أي أنه يمكن أن يلحق الضرر بسرية المعلومات أو سلامتها، أو يعيق الوصول إلى المعلومات أو يمنعه. وأسوأ من هذا أن المهاجم من الداخل إذا كان ماهراً فإنه بمقدوره أن يطمس أي آثار تدل على ارتكابه للهجوم . وأهم جوانب الأخطار التي تأتي من الهجوم الداخلي هي :

أ- مهاجمة الشبكة الداخلية للمنشأة التي يعمل فيها .

ب- مهاجمة المعلومات بالسرقة أو التغيير أو الحذف.

ج- فتح ثغرات في أنظمة الحماية التي وضعتها الجهة لتحصين أنظمة المعلومات فيها.

علاوة على ما سبق فإن المهاجم من الداخل يتمتع بمزية لا يتمتع بها المهاجمون من الخارج، وهي أنه ليس عرضة لكثير من الاحترازات الأمنية التي يتعرض لها المهاجم من الخارج. ونتيجة لذلك يمكنه القيام بأعمال يصعب على غيره القيام بها، ومن ذلك ما يلي :

أ- تغيير تهيئة (Configuration) النظام لخلق أبواب خلفية (Backdoors) ينفذ من خلالها المهاجمون مستقبلاً، مثل: أن يفتح نقطة عبور (Port) من تلك النقاط الموجودة في بروتوكول (TCP/IP) في الجهاز المستهدف[1].

ب- ردم الفجوة أو الفاصل بين الشبكات المستقلة؛ وذلك أن الجهات التي لديها معلومات مهمة جدا تسعى دوماً لفصل شبكة معلوماتها الداخلية عن شبكة الإنترنت، ونتيجة لذلك تجد أن لدى كل من هذه الجهات شبكتين: إحداهما داخلية والأخرى خارجية متصلة بشبكة الإنترنت، ولا يوضع في الشبكة الخارجية سوى المعلومات التي ترغب الجهة توفيرها للعالم الخارجي. والفصل بين الشبكتين يحمي الشبكة الداخلية من المهاجمين القادمين من الخارج، لكن المهاجم من الداخل يعمل على ردم هذه الفجوة أو إزالة هذا الفاصل، فيقوم، مثلاً، بنقل بعض المعلومات الحساسة المخزنة على الشبكة الداخلية إلى الشبكة الخارجية، أو يقوم بنقل بعض البرامج الخبيثة كالفيروسات من الشبكة الخارجية إلى الشبكة الداخلية، وكثيراً ما يكتشف في الشبكات الداخلية المعزولة فيروسات مصدرها شبكة الإنترنت. وبما أن فيروسات الحاسوب لا تستطيع الطيران في الهواء -على الأقل حتى تاريخ إعداد هذا الكتاب- فإنه لابد أن يكون شخص من داخل المنشأة قد قام بنقلها من الإنترنت إلى الشبكة الداخلية، أو عن طريق الأقراص المدمجة (CD). كما قد يقوم المهاجم من الداخل بتعطيل بعض خصائص أنظمة الحماية، أو بعبارة أخرى فتح ثغرات فيها، مهيئا بذلك رأس الجسر الذي يعبر منه المهاجمون من الخارج إلى أنظمة المعلومات التي تحاول الجهة حمايتها.

(ب) المهاجمون من الخارج

---

(1) بروتوكول (TCP/IP) هو اللغة الأكثر استخداما في الإنترنت للتخاطب وتبادل المعلومات.

نظراً لحجم التغطية الإعلامية التي تعقب الهجمات من الخارج فإننا نفترض أن القارئ قد سمع ورأى كثيرا مما قيل وكتب عن هذا الصنف، و بعض بواعث هذا النوع من الهجمات مماثلة للصنف السابق، كما أن هناك بواعث أخرى، منها: سعي المهاجم من الخارج لتحقيق أهداف سياسية أو دينية أو تجارية. ومن بواعث هذا النوع من الهجمات التجسس الصناعي أو التخريب.

الهندسة الاجتماعية
Social Engineering

[1] تعريفها وأهميتها

ليس لمصطلح الهندسة الاجتماعية (Social Engineering) معنى متفق عليه، ولكن من أقرب التعريفات أن نقول إنها استخدام المهاجم حيلا نفسية كي يخدع بها مستخدمي الحاسوب ليمكنوه من الوصول إلى أجهزة الحاسوب أو المعلومات المخزنة فيها[1]. وخلافاً لما قد يتوهم بعض الناس، فإن الهندسة الاجتماعية يجب أن تكون على رأس قائمة وسائل الهجوم التي يجب أن نحاول حماية المعلومات منها، والسبب في ذلك يرجع إلى الآتي:

(أ) إن الهندسة الاجتماعية من أنجح الوسائل التي يستخدمها المهاجم لسهولتها مقارنة بالوسائل التقنية الأخرى[2].

(ب) إن المتخصصين في مجال أمن المعلومات، وكذلك مستخدمي الحاسوب لا يعيرون خطر الهندسة الاجتماعية من اهتمامهم سوى النزر اليسير.

---

(1) مقال بعنوان: "Social Engineering: What is it, why is so little said about it and what can be done?", للكاتب (J. Palumbo) ونشر على الرابط: http://www.sans.org/infosecFAQ/social/social.htm

(2) سلسلة محاضرات ضمن دورة بعنوان: "*Hacking exposed*" ألقاها (I. Rankin) في مدينة الرياض في الفترة من 9- 12 مارس

[2] جوانب الهجمات بأسلوب الهندسية الاجتماعية

يرى بعض الباحثين[1] أن الهجمات باستخدام أسلوب الهندسية الاجتماعية يمكن أن تشن على عدة أصعدة، هي:

أ- الصعيد الحسي

يكون التركيز على موضع الهجوم والبيئة المحيطة به؛ ويدخل ضمن هذا:

(1) مكان العمل : يدخل المهاجم مكان العمل متظاهراً بأنه أحد الموظفين، أو المتعاقدين مع جهة العمل، أو عمال النظافة أو الصيانة. وإذا تمكن المهاجم من الدخول فإنه يطوف بالمكاتب لجمع ما يمكنه جمعه من كلمات المرور التي قد تكون مكتوبة على أوراق ملصقة بشاشة الحاسوب، أو لوحة المفاتيح.

(2) الهاتف : يستخدم بعض المهاجمين الهاتف لشن هجمات بأسلوب الهندسية الاجتماعية، وأكثر الأشخاص تعرضاً لهذا النوع من الهجمات هم العاملون في مراكز تقديم الدعم الفني (Help Desk). فالمهاجم، مثلاً، قد يتصل بمركز تقديم الدعم الفني هاتفياً ويطلب منه بعض المعلومات الفنية؛ وتدريجياً يحصل على ما يريده من معلومات، ككلمات المرور وغيرها. وبعد ذلك يستخدم هذه المعلومات التي يحصل عليها لشن هجمات على حواسيب المنشأة. ويرى الكاتبان أن هذا النوع من السهل تنفيذه ضد البنوك، و الشركات، والمؤسسات في مجتمعنا؛ بسبب تركيبتنا النفسية والاجتماعية التي تجعل عدداً منا يولي ثقته بسهولة لكل أحد.

(3) النفايات : قد يستغرب بعضنا إذا علم أن هذه الطريقة من أكثر الطرق شعبية بين المهاجمين الذين يستخدمون الهندسة الاجتماعية، والسر في

---

(1) مقال بعنوان: "Social Engineering Fundamentals, Part I: Hacker Tactics" للكاتب (S. Granger) ونشر على الرابط:
http://www.securityfocus.com/infocus/1527

شعبيتها أن المهاجم يستطيع جمع معلومات كثيرة ومهمة دون أن يلفت انتباه أحد.

ومن المعلومات التي توجد في النفايات كلمات المرور، والهيكل التنظيمي للشركة، ودليل هواتف الشركة، وأسماء العملين فيها، ومواعيد اجتماعات الموظفين، وفواتير الشراء... الخ. ولندلل على ما نقول نود من القارئ أن يتخيل ما يمكن أن يحدث عندما يحصل المهاجم على تقويم العام المنصرم الذي يحوي مواعيد اجتماعات موظف ما، وأماكن انعقادها، ومواضيع الاجتماعات، والأطراف المشاركة فيها. إن هذه المعلومات تضفي على المهاجم نوعاً من الشرعية. فقد يتصل، مثلاً، بسكرتير أحد الأشخاص المهمين المشاركين في أحد هذه الاجتماعات متظاهراً بأنه سكرتير مشارك آخر، ويطلب منه إرسال نسخة من التوصيات أو القرارات التي خرج بها المجتمعون إلى بريده الإلكتروني. ولاشك أن المهاجم عندما يذكر للسكرتير مكان الاجتماع، وموعد انعقاده، وأسماء بعض من حضروه، فإن السكرتير سيظن أن المهاجم هو حقاً سكرتير موظف آخر مشارك في الاجتماع، وإلا كيف عرف كل هذه التفاصيل عن الاجتماع، وهذا يجعل السكرتير يرسل للمهاجم ما طلب، ويمكن للمهاجم الاستفادة من هذه المعلومات الجديدة التي حصل عليها لشن المزيد من الهجمات للحصول على مزيد من المعلومات وهكذا.

(4) **الإنترنت**: عندما يستخدم شخص ما عدة برامج أو تطبيقات يتطلب كل منها كلمة مرور مثل: (Yahoo) و(Hotmail) وغيرها، فإنه غالباً ما يجنح إلى استخدام كلمة مرور واحدة لها جميعاً ليسهل على نفسه تذكرها. لكن المشكلة هي أنه عندما يستطيع مهاجم ما معرفة كلمة المرور هذه فإنه يصبح من السهل عليه اختراق كل التطبيقات التي يتعامل معها صاحب كلمة المرور الأصلي. ومن وسائل المهاجمين في

الحصول على كلمة المرور إلى الإنترنت، إن ينشئ المهاجم المتربص موقعاً على شبكة الإنترنت يقدم خدمات معينة، مثل: تنزيل البرامج المجانية، ولكنه يشترط على الراغب في تنزيل هذه البرامج أن يدخل رقم المستخدم وكلمة المرور. ونتيجة لما أشرنا إليه آنفاً من أن بعض مستخدمي الحاسوب يفضل استخدام كلمة مرور واحدة لكل التطبيقات التي يتعامل معها فإن كلمة المرور التي يدخلها في ذلك الموقع غالباً ما تكون هي كلمة المرور نفسها التي يستخدمها في تطبيقاته الأخرى. ومن هنا يحصل المهاجم على كلمة المرور للدخول على معلومات المستهدف المخزنة في التطبيقات الأخرى.

ومن الحيل التي غالبا ما تستخدم بعد نجاح المهاجم في اختراق شبكة الشركة، أو المؤسسة: أن يقوم المهاجم بإرسال رسالة إلى جهاز الشخص المستهدف بحيث تظهر هذه الرسالة في صورة صندوق حواري (Dialog Box)، كأنها رسالة قادمة من إداري الشبكة يطلب فيها من الشخص المستهدف أن يعيد إدخال اسم المستخدم، وكلمة المرور، مبرراً ذلك بوجود تحديث في الشبكة، أو وجود مشاكل فنية تستلزم ذلك. و إذا انطلت الحيلة على الشخص المستهدف يحصل المهاجم على كل ما يلزمه للوصول للمعلومات الخاصة بذلك الشخص.

ب- الصعيد النفسي

هذا المستوى يعنى بالمناخ النفسي المحيط بالطريقة التي ينفذ بها الهجوم. فالمهاجم يسعى إلى خلق الأجواء النفسية المناسبة لإيهام الضحية بأن المهاجم شخص موثوق به، ولديه صلاحية الاطلاع على المعلومات الحساسة للشخص المستهدف أو المنشأة المستهدفة.

[2] أساليب الهجوم باستخدام الهندسة الاجتماعية

هناك عدة أساليب للهجوم باستخدام الهندسة الاجتماعية، ولكن أشهرها ما

يلي:

أ- أسلوب الإقناع (Persuasion):

هذا هو أهم أساليب هذه الطريقة؛ ولذلك سنفصل الكلام فيه. وبادئ ذي بدء نقول إن سيكولوجية الإقناع لها جوانب متعددة أهمها[1]:

(1) **طـــرق الإقنـــاع**: تدل الدراسات التي أجريت في علم النفس الاجتماعي (Social Psychology)أن هناك طريقتين لإقناع شخص لعمل شيء ما:

(أ) طريقة الإقناع المباشرة: في هذه الطريقة يتذرع المهاجم بالحجج المنطقية والبراهين لحفز المستمع – في هذه الحالة الضحية – على التفكير المنطقي والوصول إلى نتيجة يرغب المهاجم في جر الضحية إليها.

(ب) الطريقة غير المباشرة: هنا يعتمد المهاجم على الإيحاءات النفسية، والقفز فوق المنطق، وتحاشي استنفار قدرة التفكير المنطقي لدى الضحية، وحث الضحية على قبول مبررات المهاجم دون تحليلها والتفكير فيها جدياً.

ومن الواضح أن المهاجم لا يملك، غالباً، مبررات وحججاً منطقية لإقناع الشخص المستهدف بعمل ما يرغبه, ولذلك فإنه يلجأ غالباً للطريقة الثانية، أي: الطريقة غير المباشرة، فيعمد في بداية لقائه بالضحية إلى إطلاق عبارات تستثير الشخص المستهدف نفسياً، إما ببث مشاعر الخوف، أو مشاعر الحماس في نفسه. وهذه الموجة من المشاعر النفسية تعمل على تشتيت ذهن المستهدف، وتشوش نظرته للأمور، فتضعف قدراته على التفكير والتحليل المنطقي، فيصعب عليه -تبعاً لذلك- مواجهة

(1) مقال بعنوان: "*Central and Peripheral Routes to Persuasion: An Individual Difference Perspective*" لعدد من الكتاب و نشر في مجلة: Journal of Personality and Social Psychology عام 1986م.

حجج المهاجم ومبرراته وإن كانت ضعيفة[1].

(2) **أساليب التأثير المستخدمة في طريقة الإقناع غير المباشرة:** فيما يلي نعرض أنجح الأساليب التي يُعْمِلها المهاجم ضد خصمه عندما يستخدم الأول طريقة الإقناع غير المباشرة:

(أ) **التزيي بمظهر صاحب السلطة:** إن الغالب على الناس سرعة تلبية طلبات ذي السلطة، حتى وإن لم يكن موجودا بشخصه. وقد أجريت تجربة في ثلاثة مستشفيات بالولايات المتحدة حيث ادعى الشخص الذي أجرى التجربة أنه طبيب، واتصل هاتفياً باثنتين وعشرين مكتباً من مكاتب المرضات بالمستشفيات الثلاثة، وفي كل مرة كان يطلب من الممرضة التي ترد على مكالمته أن تصرف 20مللجراما من دواء معين لمريض معين موجود في الجناح الذي يشرف عليه مكتب الممرضات الذي اتصل به الباحث. وفي هذه التجربة عدة أمور يجب أن يُنتبه إليها:

أولاً: إن المرضة لم يسبق لها رؤية الطبيب المزعوم، أو حتى الحديث إليه هاتفياً.

ثانياً: إن هذا الطبيب كان يعطيها الوصفة هاتفياً، بدلاً من الحضور شخصياً لإعطاء الوصفة كما تنص على ذلك قواعد العمل في المستشفيات التي أجريت التجارب فيها.

ثالثاً: إن العلاج الذي وصفه الطبيب المزعوم، لم يكن استخدامه مسموحاً به داخل ذلك الجناح.

---

(1) كلمة بعنوان: "The "Social Engineering of Internet Fraud", A Prepared Statement of U.S. ألقاها Jonathan J. (Rusch، من وزارة العدل الأمريكية أمام مؤتمر (INET'99) و نص الكلمة موجود على الرابط:
http://www.isoc.org/isoc/conferences/inet/99/proceedings/3g/3g_2.htm

رابعاً: إن الجرعة التي وصفها ذلك الطبيب كانت ضعف الحد الأقصى المسموح به في الأجنحة التي يسمح فيها بوصف ذلك الدواء.

ومع كل هذا فإن 95٪ من الممرضات التي جرى الاتصال بهن كن في طريقهن لتنفيذ طلبات الطبيب، لكن المراقبين المشاركين في التجربة أوقفوهن قبل تنفيذ ذلك.

(ب) **الإغراء بامتلاك شيء نادر**: إن الناس في مجملهم لديهم الرغبة في امتلاك أي شيء مهما كان إذا أحسوا أن ذلك الشيء أصبح شحيحاً، أو أنه متوفر لفترة محدودة، وهذا أمر يدل عليه الواقع المعيش، كما دلت عليه الدراسات التي أجريت في مجال علم النفس الاجتماعي. كما أن رغبتهم تزداد في امتلاك ذلك الشيء متى ما أشعروا أن قدرتهم على امتلاكه ستصبح محدودة في المستقبل. إن هذا السلوك يمكن أن يستغله المهاجم فيعرض في موقعه مثلاً شاشات توقف (Screen Savers) فيها صور مغرية، ويعطي إمكانية تحميلها من موقعه، ثم يعلن أن هذا العرض يسري لمدة محدودة فقط، ويشترط على الشخص الراغب في تحميلها أن يشترك في الموقع، ولا يحتاج الاشتراك إلى أكثر من اختيار رقم مستخدم وكلمة مرور. وهنا قد يقع الشخص المستهدف في الفخ لحرصه على تنزيل هذه الشاشات، فيدخل رقماً مستخدماً؛ وكلمة المرور قد تكون هي نفس ما يستخدمه في تطبيقات أخرى مثل البريد الإلكتروني أو قاعدة بيانات الشركة. وفي هذه الحالة يمكن للمهاجم المتستر وراء هذا الموقع الدخول إلى البريد الإلكتروني، الخاص بالضحية، أو دخول قاعدة بيانات الشركة التي يعمل فيها.

(جـ) **إبراز أوجه التشابه مع الشخص المستهدف**: إن من خصائص النفس البشرية الميل إلى من يشبهها في العرق، أو اللون، أو الاهتمامات والطباع. وإحساسنا

بوجود أوجه شبه مع شخص ما يجعلنا أقل حذراً عند التعامل معه ، لأننا لا إرادياً نعطل بعض قدراتنا على التحليل والتفكير المنطقي. وقد يوظف المهاجم هذه الخاصية البشرية لمصلحته ؛ فقبل أن يطلب من الشخص المستهدف معلومات مهمة يجمع المهاجم معلومات عن الشخص المستهدف : كمكان ميلاده ، أو الهوايات التي يمارسها ، أو نحو ذلك ، ثم يبدأ حواراً مع المستهدف حول هذه الأمور ، و يوهم المستهدف بأنه ولد في المدينة نفسها ، أو أنه يمارس الهوايات نفسها, و هذا يُشعر المستهدف بوجود أوجه شبه بينه وبين المهاجم المتربص ، فتنبني بينهما علاقة ثقة لا أصل لها ، فيسترخي المستهدف ذهنيا ، بعدها يبدأ المهاجم باستدراج المستهدف لإعطائه المعلومات التي يرغب الحصول عليها.

(د) رد الجميل: إن من خصائص النفس السوية رغبتها في رد الجميل إلى من أحسن إليها. وتزداد هذه الخاصية رسوخاً في المجتمعات ذات الصبغة القبلية والأسرية. فمن قواعد التعامل أن من أسدى إليك معروفاً – ولو لم تطلب منه ذلك ابتداء – فإنك ملزم أدبياً بمقابله ذلك المعروف بمثله أو أحسن منه وهذا خلق حسن. غير أن المهاجم قد يستغله فيقدم خدمة للشخص المستهدف ، وقد تأتي هذه الخدمة في صورة مساعدة في حل مشكلة فنية ، أو استرجاع ملف مهم حذف ، فيتولد عند المستهدف شعور أنه مدين لمن ساعده. وقد يستغل المهاجم هذا الشعور فيطلب من المستهدف مساعدته بإعطائه بعض المعلومات ، أو السماح له باستخدام جهازه – لطباعة بعض الملفات مثلاً – ، فلا يجد المستهدف بدا من رد الجميل ، مما يمكن المهاجم من زرع بعض البرامج الخبيثة ، أو الحصول على معلومات لم يكن سائغاً أن يحصل عليها.

ب– أسلوب انتحال الشخصية (Impersonation)

وتعني تقمص إنسان ما شخصية إنسان آخر ، وقد يكون هذا الآخر شخصاً

حقيقياً أو متوهما. ومن الشخصيات التي يكثر انتحالها في مجال الهندسة الاجتماعية : شخصية فني صيانة معدات الحاسوب والشبكات، وعامل النظافة، والمدير، والسكرتير. كما يكثر انتحال شخصية طرف ثالث مخول من قبل الإدارة العليا في الشركة أو المؤسسة. ولتوضيح ذلك قد يحصل المهاجم على اسم المستخدم الخاص بالبريد الإلكتروني لمدير الشركة، وهذه مسألة سهلة لأن هذا الاسم ليس سرياً. بعدها يتصل المهاجم بأفراد مركز تقديم الدعم الفني بالشركة مقدماً نفسه على أنه سكرتير المدير، مدعياً أن المدير قد كلفه بالاتصال بهم ليطلب كلمة مرور جديدة، نظراً لأن المدير قد نسي كلمة المرور السابقة، وأنه يجب إصدار كلمة المرور الجديدة فوراً، لأن المدير لديه اجتماع بعد ساعة، ويرغب في مراجعة بعض الوثائق المهمة التي أرسلها أحد المشاركين في الاجتماع إليه عن طريق البريد الإلكتروني. وإذا كان المهاجم بارعاً في تقمص شخصية السكرتير فإن أفراد مركز تقديم الدعم الفني قد يصدرون كلمة مرور جديدة للمدير ويعطونها للمهاجم المنتحل شخصية سكرتير المدير، وبذا يستطيع المهاجم الدخول إلى البريد الخاص بمدير الشركة.

وتقمص الشخصية يسهل في الشركات والتجمعات الكبيرة التي لا يعرف أفرادها بعضهم بعضاً. و من القصص الواقعية ما حدث لأحد مؤلفي هذا الكتاب عندما كان يدرس إحدى مواد الدكتوراه، إذ أرسل المدرس أسئلة الواجب بالبريد الإلكتروني، وطلب إرسال الردود عليها بالبريد الإلكتروني، ووضع موعداً لا يقبل أي إجابات بعده. وقبيل حلول الموعد النهائي بساعتين وصل بريد إلكتروني إلى عدد من الطلاب من شخص تقمص شخصية مساعد مدرس المادة — وهو شخص حقيقي، غير أن كثيرا من الطلاب لا يعرفونه — يطلب من الطلاب أن يرسلوا إجابتهم إلى بريده واستخدم اسماً وهمياً. تبين بعد ذلك أن مرسل هذا البريد كان أحد طلاب

المادة، لكنه لم يتمكن من حل بعض الأسئلة، وأراد أن يرى كيف حلها الطلبة الآخرون. ولفرط ذكاء المهاجم لم يرسل البريد إلى جميع الطلاب بل اكتفى بإرساله لبعضهم حتى لا يفتضح أمره.

جـ – أسلوب المداهنة

عند التأمل في الشخصيات التي يكثر انتحالها، وذكرناها في الفقرة السابقة، يتضح للعيان أنها في الأعم لأناس تدعمهم سلطة قوية داخل الشركة أو التجمع – كالفصل الدراسي–. والمهاجم المنتحل لإحدى هذه الشخصيات يعلم يقيناً أن كثيراً من موظفي الشركة أو أعضاء التجمع يسعون بشتى السبل لخلق صورة حسنة عن أنفسهم عند رؤسائهم. ولذلك فإن بعضهم لن يتردد في تقديم المعلومات التي يطلبها المهاجم الذي ينتحل شخصية إنسان ذي سلطة أو ذي صلة بصاحب سلطة داخل الشركة أو المؤسسة.

د– أسلوب مسايرة الركب

هذا مسلك اجتماعي يملي على الإنسان ألا يتخذ موقفاً مغايراً لما عليه الآخرون تجاه مسألة ما. والمهاجم إذ يدرك هذا فإنه سيسعى جاهداً لاستغلاله. فعلى سبيل المثال يمكن أن يقدم المهاجم نفسه للمستهدف على أنه إداري شبكة تابع لشركة تقدم الدعم الفني لمؤسسة ما، ونظراً لوجود نسخة جديدة من برنامج ما فإنه قد قام بتثبيت النسخة الجديدة في أجهزة باقي الموظفين في الشركة، ثم يطلب من الموظف المستهدف السماح له بتثبيت النسخة الجديدة لديه. إن هذه القصة تولد شعوراً خفياً لدى المستهدف أنه مادام قد قام بتركيب النسخة الجديدة لدى بقية الموظفين فلِمَ أمنعه أنا من ذلك، وهذا يتيح للمهاجم فرصة تثبيت برامج خبيثة كحصان طروادة، مثلاً، في جهاز المستهدف.

هـ– أسلوب الهندسة الاجتماعية العكسية (Reversed Social Engineering)

هذه إحدى الطرق المتقدمة لكسب ثقة المستهدفين، ومن ثم الحصول على المعلومات. وتقوم هذه الطريقة على اختلاق موقف يُظهر المهاجم في صورة صاحب سلطة إدارية أو فنية، فيتوجه إليه المستهدفون بالأسئلة ويطلبون منه المساعدة ويتلقون منه التعليمات. وقد ذكر بعض الباحثين[1] أن تنفيذ هذه الطريقة يمر بثلاث مراحل:

(1) افتعال الموقف.

(2) إبراز المهاجم نفسه على أنه الشخص ذو المعرفة أو الصلاحية اللازمة للتعامل مع الموقف.

(3) تقديم المساعدة.

ولتوضيح المسألة نضرب المثال التالي: يقوم المهاجم بتخريب متعمد لشبكة المعلومات في أحد مكاتب الشركة مثلاً فتنقطع الخدمة عن بعض أو كل الموظفين، وهذه مرحلة افتعال الموقف. و يجب أن لا يظن أحد أن القيام بمثل هذا التخريب أمر صعب، فكل ما يُحتاج إليه هو سحب الكيبل الموصل بين المقسم وباقي الشبكة، وغالبا ما يكون هذا المقسم في مكان عام يمكن لأي شخص الوصول إليه. ووسط هذه المعمعة يظهر المهاجم بصورة المنقذ، فيقدم نفسه على أنه أحد أعضاء فريق الدعم الفني وأنه سيقوم بإنقاذ ما يمكن إنقاذه، وتأتي بعد هذا المرحلة الثالثة وهي مرحلة تقديم المساعدة إذ أن الموظفين سيتوجهون إليه بالأسئلة عما إذا كانوا سيفقدون الوثائق التي كانوا يعملون عليها لحظة انقطاع الشبكة، وهل يحتاجون إلى تغيير كلمة المرور وكيف يمكن معاودة الاتصال بالشبكة وهلم جرا. وهنا يستطيع المهاجم الحصول على المعلومات التي يريدها، وإذا كان المهاجم ذكياً فإنه سيقوم بإصلاح الشبكة بسرعة قبل

(1) مقال بعنوان: "Methods of Hacking:Social Engineering" للكاتب (R. Nelson) ونص المقال موجود على الرابط:
http://zeth.kodslav.org/security/dokumentation/dokumentation/soceng/socialeng.html

أن ينتبه لانقطاعها أعضاء الدعم الفني الحقيقيون، وإذا أفلح في فعل ذلك فسيكون قد نجح في اختراق نظام معلومات الشركة دون أن يشعر بذلك أحد.

الخلاصة

الهندسة الاجتماعية هي إعمال الحيل النفسية لخداع مستخدمي الحاسوب للوصول إلى المعلومات المخزنة فيها، وهي أسهل الأساليب و أكثرها فعالية لأنها تهاجم العنصر البشري الذي هو أضعف نقطة في منظومة حماية المعلومات، و لذا يجب أن تكون على رأس قائمة المعنيين بحماية المعلومات.

كلمــة الـمــرور
Password

[1] تعريفها وأهميتها

هل تعرف لماذا استحدثت كلمة المرور؟ إنه هو السبب نفسه الذي من أجله استحدث مفتاح البيت!. إذاً فإن هناك عاملاً مشتركاً بين كلمة المرور والمفتاح، كلاهما يمثلان أداة تخول الشخص للدخول لمكان خاص لا يدخله إلا أشخاص معينون. كلمة المرور تثبت للنظام بأنك فعلاً أنت من تدعي بأنك هو. كلمة المرور تحمي بيانات هامة مثل: سجلاتك المالية والصحية، ووثائقك وأسرارك الشخصية، وغيرها من المعلومات الحساسة الخاصة بك، أو عملك، أو بلادك. إنها أيضا تتعدى حماية البيانات إلى حماية الأفعال، مثل: القدرة على الشراء والبيع عن طريق الإنترنت. تخيل لو أن أحداً ما حصل على كلمة المرور الخاصة بحسابك البنكي على موقع البنك على شبكة الإنترنت، ألا يمكنه أن يقوم بتحويل أموال من حسابك! تخيل لو أن موظفاً ما حصل على كلمة المرور الخاصة ببرنامج الرواتب، ألا يمكنه أن يزيد من راتبه! تخيل لو أن طالبا حصل على كلمة المرور لكشف الدرجات، ألا يمكنه أن يعطي نفسه الدرجات الكاملة! بالتأكيد نعم وغيرها من الاحتمالات والحوادث كثير. إذن **قيمة كلمة المرور بقيمة ما تحميه**. فالحقيقة هي أن أول باب يطرقه المهاجم هو محاولة الحصول على كلمات المرور الضعيفة. كلمة المرور هي إحدى الطرق وأرخصها للتحكم بالدخول للنظام، لذا يتحتم علينا ثلاثة أمور:

* الاختيار الأمثل لكلمة المرور لكي لا تكون سهلة التخمين.
* المحافظة عليها وعدم اطلاع الغير عليها.
* تغييرها دورياً.

[2] تاريخ كلمة المرور

عند بداية اختراع الحواسيب كانت هناك حاجة للتحكم باستخدام تلك الحواسيب لمنع المستخدمين غير المصرح لهم بالاستخدام. فاستحدث ما يسمى باسم المستخدم (user name)، مثل :

User name
Mohammed
Abdullah
Khaled

ولكن مع مرور الوقت وكثرة المستخدمين اتضح أن اسم المستخدم غير آمن، من حيث إنه بمعرفة اسم المستخدم – وهو سهل المعرفة - يمكن الدخول للنظام. لذلك بحثوا عن طريقة يطورون بها اسم المستخدم لحماية الدخول للنظام. لقد استحدثوا ما يسمى بكلمة المرور، والتي تتميز بالمواصفات التالية :

* مرتبطة وخاصة باسم المستخدم.

* مكونة من كلمة أو أرقام أو كليهما، ولا يعرفها إلا المستخدم، فهي أكثر سريةً من اسم المستخدم.

* قد تتشابه مع غيرها من كلمات المرور لمستخدمين آخرين.

مثال على التطور الجديد :

User name	Password
Mohammed	1234
Abdullah	ATF3
Khaled	ATF3

كما تلاحظ أن كل مستخدم ارتبطت به كلمة مرور خاصة به لا يعرفها غيره، وأن كلمات المرور قد تتشابه ما دام أن اسم المستخدم مختلف. إذن فالتطور الجديد ألزم المستخدم بإدخال اسم المستخدم، ثم كلمة المرور كما في شاشة الدخول في الشكل التالي :

System X
Log On
USER NAME Khaled
PASSWORD ************

الشكل رقم (4): شاشة الدخول.

أكثر الأنظمة تتطلب صحة اسم المستخدم، وكلمة المرور معاً. فنظام ويندوز –مثلاً– يطلب اسم المستخدم والذي عادةً ما يتكون من كلمة، وموقع بريد هوت ميل Hotmail يطلب اسم المستخدم والذي يتكون من عنوان البريد الإلكتروني. كثيراً ما يقال لي: "إن النظام لم يسمح لي بالدخول، مع أني أدخلت كلمة المرور الصحيحة!". لكن يتضح لي في هذه الحال أنه بالفعل أدخل كلمة مرور صحيحة، ولكن لم يقم المستخدم بإدخال اسم المستخدم، أو أن اسم المستخدم المكتوب هو لشخص آخر.

والخلاصة هي أن الدخول للنظم الآمنة يتطلب معلومتي، هما: (اسم المستخدم وكلمة المرور)، وأن كلمة المرور لابد من إخفائها عن الجميع.

[3] الأخطار التي تكتنف استخدام كلمات المرور

ذكرنا في الجزء السابق أن أول باب يطرقه المهاجم هو محاولة الحصول على كلمات المرور الضعيفة، في هذا الجزء سنعرض لك طرق حصول المهاجم على كلمات المرور، وهي كالتالي:

* بتصديع كلمات المرور الضعيفة.
* باستخدام الهندسة الاجتماعية.
* بالبحث والتصنت التقليدي أو الحديث.

[4] تصديع كلمات المرور الضعيفة

قد تفاجأ عندما تكتشف أن عملية اكتشاف كلمات المرور الضعيفة عملية سهلة جداً كما سنوضحها في هذا الجزء. لذلك فإن أول ما يقوم به مهاجم النظام هو محاولة الحصول على كلمات المرور الضعيفة بتصديعها، وهو ما يسمى: cracking ، وهناك برامج خاصة لهذا الغرض تعتمد على عدة طرق نسردها بإيجاز:

*** التصديع باستخدام كلمات القاموس أو المعجم**

في هذه الطريقة يقوم المهاجم بمحاولة الدخول للنظام بكتابة كلمة مرور مكونة من أحد كلمات القاموس أو المعجم، فإن لم تصلح استخدم غيرها حتى يستطيع الدخول، طبعاً إذا كانت كلمة المرور هي في الأصل مكونة من أحد كلمات المعجم مثل: شمس، ريال، فلسطين، عبدالرحمن...إلخ. لكن ليست بالضرورة كلمات المعجم التقليدي بل يتعدى ذلك إلى محاولة كلمات مرور دارجة مثل 123، 2000.

*** التصديع باستخدام الطريقة الاستقصائية Brute Force**

بعض كلمات المرور لا تنتمي للقاموس، أو ليست كلمة معروفة مثل: E3، في هذه الحالة فإن الطريقة السابقة لن يمكن من خلالها معرفة كلمة المرور تلك، حتى ولو كانت ضعيفة. لذلك يتحتم في هذه الحالة استقصاء جميع الاحتمالات، حتى نصل إلى كلمة المرور. فمثلاً لإيجاد الكلمة السابقة فإنه يلزم المرور بالطرق التالية حتى نصل إليها:

AA, AB, AC…AZ, A0, A1, A2…A9
BA, BB, BC…BZ, B0, B1, B2…B9

.EA, EB, EC…EZ, E0, E1, E2, E3

فالملاحظ أننا مررنا بجميع الاحتمالات السابقة لـ E3 حتى وصلنا إليها.

*** بدمج الطريقتين**

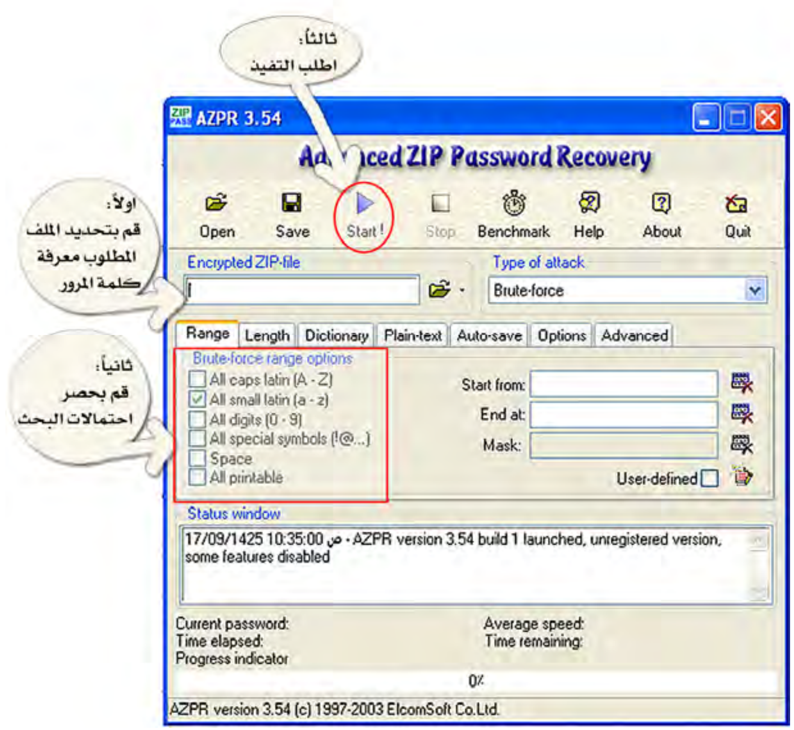
في هذه الطريقة تستخدم كلمات القاموس مع تجربة جميع الاحتمالات على الكلمة مثل : CAT, CAT0, CAT1, CAT2...CAT9.

تعتبر طريقة استخدام القاموس (قائمة الكلمات) سريعة نوعاً ما، لأن عدد الكلمات ليس كثيراً (أكثر من مليون كلمة بالنسبة للغة الإنجليزية)، وكذلك لوجود الحواسيب السريعة التي يمكن من خلالها محاولة استخدام أكثر من خمسة عشر مليون كلمة مرور في الثانية. لكنها محدودة بكلمات القاموس. أما طريقة استخدام جميع الاحتمالات فإنها ممتازة، كونها لا تدع احتمالاً إلا استخدمته، لكن مشكلتها أن تصديع كلمات المرور الطويلة قد يحتاج إلى أيام أو شهور، وفي بعض الأحيان إلى سنوات، خاصة مع كلمات المرور المكونة من أكثر من ثماني خانات، وتحوي خليطاً من الأرقام، والحروف، والرموز.

و يوجد عدد من البرامج التي تصدع كلمات المرور، ولنأخذ واحداً منها وهو برنامج Advanced ZIP Password Recovery (AZPR)، والذي يمكن تنزيله من الموقع : http://www.elcomsoft.com

يتاح من خلال هذا البرنامج، بتصديع الملفات المضغوطة بصيغة (ZIP) والمحمية بكلمة مرور. و يتميز هذا البرنامج بسرعة المحاولات، فسرعته تصل إلى 6 ملايين محاولة في الثانية الواحدة!.

لنأخذ الآن مثالاً على سهولة تصديع كلمة المرور واكتشافها لملف مضغوط (ZIP) محمي بكلمة مرور ضعيفة. أخذنا ملفاً وقمنا بضغطه، ومن ثم حمايته بكلمته مرور (sami). الملف الآن لا يستطيع فتحه إلا من لديه معرفة بكلمه المرور، أو هكذا يظن من قام بحمايته. لكن الحقيقة هي أن الملف يمكن فتحه بدون معرفة كلمة المرور وبكل سهولة أيضا. استخدمنا برنامج AZPR، وأشرنا للملف المضغوط المحمي، ثم طلبنا من البرنامج إيجاد كلمة المرور الخاصة بالملف.



الشكل رقم (5): استخدام برنامج (AZPR).

وبعد الضغط على زر Start! شاهد على ماذا حصلنا :

Password successfully recovered !

Advanced ZIP Password Recovery statistics:

Total passwords	241
Total time	12ms
Average speed (passwords per second)	20,083
Password for this file	ii
Password in HEX	69 69

Save... ✓ OK

الشكل رقم (6): الحصول على كلمة المرور.

لقد حصلنا على كلمة المرور الخاصة بالملف في غضون 12 مللي ثانية، أي أقل بكثير من الثانية. لقد بذلت 241 محاولة للوصول إلى كلمة المرور، كذلك قدم لنا البرنامج كلمة مرور (ii) غير التي حددناها مسبقا عند ضغط الملف، وهي (sami)، ولكن حتى كلمة المرور التي قدمها البرنامج استطعنا فتح الملف بها. هذا يدل على أنه يوجد أكثر من كلمة مرور - وغالباً أسهل أو أضعف من كلمة المرور الأساسية-، يمكن بواسطتها فك التشفير. أرأيت سهولة تصديع كلمة المرور الضعيفة ةاكتشافها. لذا احرص على اختيار كلمة مرور قوية يصعب على المهاجم تصديعها، وقم بتغييرها دورياً. لأنه كلما كانت كلمة المرور أقوى (أي أطول وتحتوي على تشكيلة من الحروف والأرقام والرموز) كان وقت تصديعها أطول، وقد يصل إلى سنين.

[5] استخدام الهندسة الاجتماعية

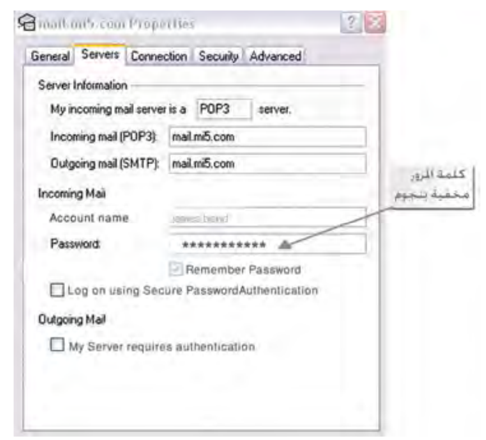
الهندسة الاجتماعية -كما هو مبين بتفصيل أكثر في فصل الهندسة الاجتماعية- هي عملية الحصول على كلمة المرور بالتلاعب على الشخص الضحية، أو بمعرفة معلومات شخصية مثل اسم أبناء الضحية، تاريخ الميلاد، الأكلة المفضلة، والتي قد تتكون منها كلمة المرور مثل Ahmed, 1970, Kabassah.

[6] البحث والتصنت التقليدي أو الحديث

من أمثلة البحث والتصنت التقليدي هو الوقوف خلف الضحية عند كتابته كلمة المرور، أو البحث عن كلمة مرور الضحية مكتوبةً تحت لوحة المفاتيح. أما البحث والتصنت الحديث فهو باستخدام التقنية الحديثة، مثل تركيب برنامج صغير يسجل جميع الأحرف والأرقام المدخلة عن طريق لوحة المفاتيح، أو مراقبة جميع المعلومات الخارجة من الحاسوب إلى الشبكة، وهذه الطريقة مشروحة بشكل أكثر تفصيلاً في موضع آخر من الكتاب.

ويمكن أيضا معرفة كلمات المرور بطريقة أخرى، فعند تخزين كلمة المرور في

النظـام: كالـدخول إلى الإنترنـت، أو بريـدك الشخصـي، أو بعـض الإعـدادات الشخصية، فإنك عندما تعاود الدخول أو الاتصال تظهر كلمة المرور المخزنة، ولكن بهيئة نجوم (أو دوائر صغيرة كما في ويندوز اكس بي) للتعتيم فقط، كما في الشكل رقم (7).



الشكل رقم (7): كلمة المرور في ويندوز إكس بي.

هل تعتقد أن هذا التعتيم آمن؟ للأسف لا، فهناك برامج متاحة لمعرفة ما تحت هذا التعتيم، وهي برامج لمعرفة كلمات المرور المنسية، وكذلك يمكن أن تستخدم استخداماً غير نظامي لمعرفة كلمات مرور غيرك المخزنة على أجهزتهم. خذ هذا السيناريو: قدمتَ إلى أحد المكاتب في شركتك وقت الغداء، وقد نسي (أو لم يتعود) صاحب الجهاز إقفاله، أو حمايته بكلمة مرور، عندها تمكنت من تحميل برنامج صغير من على قرص أو سواقة USB الصغيرة على جهاز الشخص الغائب، وبحثت عن المواضع التي توفر تسجيل كلمات المرور للاستخدامات اللاحقة، وتقدمها بشكل معتم على هيئة نجوم مثل الشكل السابق. ثم استخدمت، البرنامج الذي حملته لمعرفة كلمات المرور تلك كما في الشكل رقم (8) :



الشكل رقم (8): معرفة كلمة المرور المخفية.

هناك أكثر من برنامج لمعرفة كلمات المرور المعتمة، ولكنا استخدمنا في هذا المثال برنامج SeePassword (1) الذي يحاكي شكل العدسة المكبرة، وبتمرير البرنامج (العدسة) على كلمة المرور المعتمة يمكنك معرفة كلمة المرور بكل سهولة. جرب بنفسك!.

[7] الاختيار الأمثل لكلمة المرور

بعد معرفة كيفية تصديع المهاجم لكلمات المرور، يجب عليك تكوين كلمة مرور قوية لا تكون صيداً سهلاً لبرامج التصديع. ولتكوين كلمة مرور قوية عليك اتباع الخطوات التالية:

---

(1) http://www.seepassword.com/.

* لا تكون كلمة المرور من كلمة واحدة مثل : Makkah, Sami, Alhilal

* لا تضمن كلمة المرور معلومات شخصية مثل تاريخ الميلاد، واسم بلد، وصديق، أو لون تحبه.

* لا ينبغي ألا تقل كلمة المرور عن 10 خانات، لأن السرعة الفائقة للحواسيب الحديثة تجعل من تصديع كلمة المرور واكتشافها أمراً يسيراً.

* كون كلمتك من خليط من الحروف (الصغيرة والكبيرة)، والأرقام والرموز ، فكلما كان الخليط أكثر كان تصديع كلمة المرور أصعب. لنأخذ مثالاً :

كم محاولة نحتاجها حتى نصدع كلمة المرور ونعرفها؟.

مكونات كلمة المرور	**عدد المحاولات لكلمة المرور**		**عدد المحاولات لكلمة مرور مكونة من 10 خانات**
	مكونة من خانة	**مكونة من خانتين**	
أرقام فقط	10	100	10,000,000,000
حروف إنجليزية فقط ذات حالة واحدة (صغيرة أو كبيرة)	26	676	141,167,095,653,376
رموز فقط (>,<,!, @,#,%,^,&, *,$) ولنفرض أن عددها 10	10	100	10,000,000,000
أرقام أو حروف أو رموز	46	2116	42,420,747,482,776,576

لاحظ كيف أن محاولات تصديع كلمة المرور ومعرفتها تكون أكثر عندما تتضمن كلمة المرور خليطاً من الأرقام والحروف (الصغيرة و الكبيرة) والرموز. لذا عليك استخدام كلمة مرور مكونة من خليط ، وتفادي إضافة الرموز في نهاية كلمة المرور مثل : hwrqtdy@&a ، بل اجعلها : h@wrq&tdya.

* استخدم اختصار جملة ، مثل اختصار عبارة أو جملة : " I live in Emirate Since 1990" في "1Lv@3$I99O". لاحظ كيف استبدلنا حرف I برقم 1 ، واستخدمنا حرف L بصفته الكبيرة واستبدلنا in بحرف @ ، وS بـ $ ، و رقم 1 بحرف I ، و رقم 0 بحرف O. وتسمى هـذه عبـارة المرور (Passphrase) ، وتتميز هذه الطريقة بإمكانية تكوين كلمة مرور قوية ، ويسهل تذكرها.

* تجنب تضمين اسم المستخدم داخل كلمة المرور.

[8] التعامل الصحيح مع كلمة المرور

بعد معرفة كيفية حصول المهاجم على كلمات المرور ، لابد من تفادي الطرق التي تسهل على المهاجم الحصول عليها ، وذلك باتباع الآتي :

* لا تطلع غيرك على كلمة المرور الخاصة بك ، حتى لو كان مدير النظام System Administrator .

* لا تكتبها ، لكن إذا اضطررت لذلك فاحفظها في مكان آمن. و في حال انتهاء استخدامها أتلفها بطريقة صحيحة حتى لا يستطيع غيرك معرفتها حتى وإن كانت كلمة المرور غير صالحة ، فإن المهاجم يمكن أن يتعرف على نمط اختيارك لكلمة المرور ، ويستطيع بذلك أن يتوقع كلمات المرور الأخرى سارية المفعول الخاصة بك.

* غيّر كلمة المرور دورياً حسب أهمية النظام المراد الدخول إليه (تقريباً شهر إلى شهرين للحسابات البنكية ، و 3-4 شهور لحسابات الشركة) ، لأنه قد يحدث في بعض الأحيان أن يُخترق جهاز الخادم (Server) الذي تُخزن فيه جميع كلمات المرور وأنت

لا تعلـم. -أو كمـا أوضـحنا سـابقاً- قـد تـنجح طريقـة تصـديع كلمـة المرور باستخدام الطريقـة الاستقصائية Brute Force ، حتى مع كلمات المرور غير القصيرة بعـد مـرور فـترة زمنية كافية لاستخدام جميع الاحتمالات. لذا فتغييرك كلمة المرور يفسد على المهـاجم الجهد الكبير الذي بذله ، لأنه يحاول الحصول على كلمة مرور قديمة !.

* لا تستخدم كلمة مرور واحدة مع عدة حسابات وأنظمة ، لأنـه إذا تم تصـديع كلمـة مـرور أحـد الحسـابات أو الأنظمـة اسـتطاع المهـاجم بهـذا أن يصـل إلى جميـع حساباتك وأنظمتك ، وذلك لتشابه كلمات المرور.

* لا تخزن كلمة المرور على الحاسوب (خيار الاحتفاظ بكلمة المرور) ، لأنـك لا تعلم مدى أمان تخزين كلمـة المرور في الحاسـوب. كـذلك لا تعتمـد عـلى الـبرامج الـتي توفر لك تذكر كلمات مرورك بدلاً من تذكرك لها ، مثل : برنامج Gator لأن أكثر تلـك البرامج برامج تجسسية ولا تؤتمن ، فكيف تأمن شخصاً غريباً على مفـاتيح بيتـك لمجـرد أنه يفتح الباب لك كلما أردت الدخول !.

* غير كلمة المرور المقدمة إليك فوراً عند فتح حساب جديد.

* راجع أنظمة التعامل مع كلمة المرور الخاصة بمنظمتك ولوائحها وتقيد بها.

[9] المقاييس الحيويةBiometrics

لا يعتمـد التحقـق الأدق مـن هويـة الشـخص عنـد الـدخول للنظـام عـلى كلمـة المـرور ، بـل هنـاك تقنيـات حديثـة تسـمى : Biometrics (القياسـات الحيويـة) تتميـز عـن كلمات المرور بالآتي :

* إنها لا تحتـاج إلى تـذكر كلمـات ، بـل تحتـاج إلى صـفات بشـرية للتعـرف عـلى المستخدم.

* يصعب إعطاء غيرك هذه الصفات للدخول للنظام.

* هذه الصفات دائماً مع الشخص ، ويصعب نسيانها أو انتفاؤها عنه.

من أنواع هذه التقنيات

* تقنية التعرف عن طريق بصمة الأصابع.
* تقنية التعرف عن طريق اليد.
* تقنية التعرف عن طريق الوجه.
* تقنية التعرف عن طريق شبكية العين.
* تقنية التعرف عن طريق الصوت.

كل واحدة من الطرق السابقة لها درجة من الأخطار والتكاليف والاعتمادية. أحد أهم عوائق استخدام هذه التقنيات هي التعدي على خصوصية الأشخاص، أو صفاتهم. ومن العوائق أيضاً الخوف من تأثير تلك التقنيات في الإنسان، مثل تقنية التعرف عن طريق شبكة العين، خاصة أن التقنية حديثة ولم يتم دراسة آثارها البعيدة المدى. كذلك أحد العوائق هي التكلفة المرتفعة بالمقارنة بكلمات المرور. لكن نخلص إلى القول إن اختيار إحدى التقنيات على الأخريات يعتمد على عوامل عدة، من بينها: التكاليف، وحساسية النظام المراد الدخول إليه، وسهولة التطبيق والمتابعة.

الخلاصة

كلمة المرور هي أحد مكونات منظومة حماية المعلومات فهي تساعد على التحقق من هوية المستخدم، و فاعليتها تعتمد على درجة انضباط العنصر البشري في اختيار كلمة المرور و التعامل معها وفق الأساليب الصحيحة. وهناك وسائل بديلة أو مكملة لكلمة المرور، ولكن لكل من هذه الوسائل ما يحف به من أخطار، وما يطلبه من تكاليف.

البرامج الخبيثة
Malicious Codes أو Malware

من البشر من هم بناؤون ؛ كما أن منهم هدّامون. منهم من يطور برامج مفيدة هادفة ، ومنهم من يطور برامج خبيثة ، بل إن بعض البرامج يمكن استخدامها لعمل صالح وضار حسب من يستخدمها ويستفيد منها. وفي هذا الفصل سنتطرق لتعريف البرامج الخبيثة وذكر أنواعها بالتفصيل ، وكيفية الوقاية والتخلص منها.

فالبرامج الخبيثة هي أي برنامج يكون كل مهامه أو أحدها عمل خبيث من تجسس أو تخريب ، أو استنزاف للموارد (الوقت ، المعالج ، الذاكرة ، وحدة التخزين ، سعة النقل الشبكي وغيرها....).

[1] دوافع تطوير البرامج الخبيثة

* لمجرد أن يثبت الشخص لنفسه أو لغيره قدرته على تطوير برامج تستطيع الاختراق أو التجسس أو التخريب. وهذا غالباً ينتشر بين صغار السن أو المبتدئين.

* للتجسس الصريح ، وسرقة المعلومات ، سواء على مستوى أفراد ، أو شركات ، أو دول. هناك شركات تسعى للحصول على معلومات سرية خاصة بالشركة المنافسة ، وهناك دول تتجسس على غيرها من الدول لجمع معلومات مهمة تمس أمنها. بل إن المباحث الفدرالية الأمريكية طورت برنامج خبيثاً لتتجسس على الأفراد دون علمهم.

* الانتقام من أفراد ، أو شركات ، أو دول. مثلاً : نجد عديداً من المطورين يحاولون النيل من شركة ميكروسوفت لاستحواذها وسيطرتها على الأسواق البرمجية.

* للابتزاز. فهناك من الخبثاء من يقوم بسرقة معلومات مهمة لشركة ، ثم يقوم بمساومة الشركة على تلك المعلومات.

* التسويق التجاري واستنزاف ا .ما تكون الإعلانات التجارية غير

مرغوب فيها وإجبارية، وتستنزف موارد الجهاز من معالج، وذاكرة، ووحدة تخزين، وسعة نقل الشبكة، فإن تلك البرامج تعد خبيثة.

[2] أنواعها

هناك أنواع عديدة للبرامج الخبيثة، منها: الخبيث الصريح، ومنها ما يكون من ضمن أعمالها تأثير سلبي غير معلوم للمستخدم، مثل: استخدام مصادر الحاسوب (الذاكرة والمعالج)، والتجسس التجاري. وبهذا التقسيم يمكننا إدراج برامج الإعلانات Adware ، وبرامج متابعة تصرفات المستخدم أو التجسس البسيط Spyware تحت البرامج الخبيثة؛ لأنها إما أن تستهلك موارد الحاسوب والشبكة، أو تتابع تحركاتك دون علمك، وهذا بحد ذاته عمل خبيث. وفيما يلي بعض أنواع البرامج الخبيثة.

* الفيروسات Viruses .
* الديدان Worms .
* الخدع أو البلاغ الكاذب Hoax .
* الأحصنة الطروادية Trojan Horses.
* رسائل الاصطياد الخادعة Phishing, Scam.
* برنامج تجسسي Spyware .
* برنامج إعلاني Adware.
* صفحات فقّاعية أو انبثاقية Popup .
* برنامج تسجيل نقرات لوحة المفاتيح Keystroke Logger.

[3] طرق الإصابة بها

هناك عدة طرق للإصابة بالبرامج الخبيثة بشكل عام منها:

* **وسائط التخزين**: قد تنتقل البرامج الخبيثة من حاسوب مصاب إلى آخر سليم بواسطة وسائط التخزين التي تنقل الملفات والبرامج. و من أمثلة الوسائط: القرص

المرن Floppy Disk ، القرص المدمج CD، ووحدة التخزين الخارجي، ووحدة تخزين USB، و كروت الذاكرة Memory Cards.

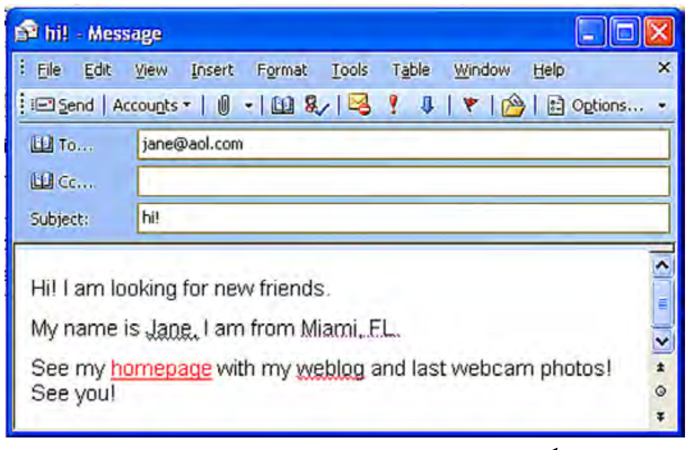
* **عن طريق البريد الإلكتروني**:أصبح البريد الإلكتروني من النواقل الأكثر أهمية في نقل البرامج الخبيثة، وذلك لانتشاره الواسع بدون قيود أو حدود جغرافية. وهناك عدة أشكال للرسائل التي تحمل البرامج الخبيثة، منها:

* **عن طريق المرفقات** Attachments : يمكن أن يرسل لك أحد ما رسالة تحتوي على مرفق لبرنامج يدّعي فائدته، وعند فتحه يشغل البرنامج كما وعدك، ولكن في الوقت نفسه يصيب جهازك ببرنامج خبيث. ولإضفاء قدر من المصداقية على الرسالة قد ينتحل المهاجم العنوان البريدي الخاص بأحد أصدقائك، معتمداً على أنه لا يساورك شك بأن صديقك سيرسل لك برنامجا خبيثاً أو يَحتال عليك. أو قد يوهمك بأنه مُرسل من شركة ميكروسوفت، ويحتوي على تحديث لنظام التشغيل لسد إحدى الثغرات الأمنية كما يدّعي. تأكد أن شركة ميكروسوفت لن ترسل تحديثاً بواسطة ملف مرفق في رسالة بريدية. وللعلم فإن بعض البرامج الخبيثة إذا أصابت جهازك تقوم بإرسال رسالة بريدية إلكترونية باسمك موجهة لجميع العناوين البريدية التي في دفتر العناوين الخاص بك، وتجعل مرفقاً مع الرسالة ملفاً يحوي نسخة من البرنامج الخبيث، وبهذا تنتشر العدوى إلى أجهزة معارفك.

* **عن طريق مجـرد قـراءة الرسـالة**: بعض برامج البريد الإلكتروني- مثل Microsoft Outlook Express – تحتوي على ميزات لتسهيل عرض الرسائل، غير أنها تحتوي على ثغرات أمنية تتيح- بمجرد تصفح الرسالة البريدية القادمة- ؛ تحميل الملفات المرفقة مع الرسالة أو تشغيلها، والتي قد تكون في بعض الأحيان برامج خبيثة.

* **عن طريق رابط في الرسالة**: تحتوي بعض الرسائل البريدية على رابط يحثك على الذهاب إليه، كأن يدّعي بأنه رابط لصورته أو لصورتها، أو أنه تحديثات لسد

ثغرات أمنية، أو غيرها من الخداع. الرسالة التالية هي أحد الأمثلة على الرسائل المحتوية على روابط. الروابط بحد ذاتها لا تؤثر، لكن المشكلة تكمن في الموقع المحول إليه الرابط، فالروابط تؤدي إلى مواقع تستغل ثغرة أمنية في متصفح الإنترنت، وتقوم باستغلال الثغرة في تحميل برنامج خبيث آخر أو تشغيله.



الشكل رقم (9): الإصابة عن طريق رابط الرسالة

* **تصفح مواقع مشبوهة:** يحتوي متصفح الإنترنت على عديد من الثغرات الأمنية التي غالباً ما يتجاهل المستخدم سدها وإصلاحها. وبعض المواقع المشبوهة تستغل تلك الثغرات في الوصول لجهاز المستخدم، وتحميل البرامج الخبيثة عليه.

* **المراسل الآني Instant Messenger:** من أمثلته (MSN Messenger, Yahoo Messenger, ICQ). وهي برامج للتخاطب، وتناقل الملفات بشكل مباشر مع الأصدقاء أو الغرباء. ولبرامج المراسل الآني مشكلتان: أولاهما: أنك لا تستطيع الجزم بأن من يخاطبك على برنامج المراسل هو صديقك، لأنه يمكن أن يسرق أحد المخربين اسم المستخدم، وكلمة المرور لصديقك على برنامج المراسل، ثم ينتحل شخصية

صديقك، ويستغل الثقة بينكما ويرسل لك برنامجاً خبيثاً. أما المشكلة الأخرى فهي الثغرات الأمنية لبعض برامج المراسل الآني، خاصة القديمة منها التي يستطيع المهاجم من خلالها اختراق جهازك وبث البرامج الخبيثة فيه.

* **المنافذ المفتوحة Open ports**: عندما يتصل جهازك بالشبكة فإنه يتخاطب من خلال منافذ معينة لكل تطبيق. فمثلاً عندما تتصفح الإنترنت فأنت تمر من خلال منفذ رقم 80، وعندما تريد إرسال بريد إلكتروني تستخدم منفذ رقم 25. يستطيع المهاجم من خلال ثغرات أمنية على بعض التطبيقات المعتمدة على بعض المنافذ تمرير برنامج خبيث إلى جهازك دون علمك.

* **تحميل برامج من الإنترنت Downloading**: عند تحميل برامج من على الإنترنت قد تحتوي على برامج خبيثة مبطنة بها.

[4] طرق الوقاية

قديماً قيل "الوقاية خير من العلاج". وهناك عديد من الإجراءات والنصائح التي يجب إتباعها في حياتك اليومية لتفادي الإصابة بالبرامج الخبيثة، منها:

* لا تفتح أي ملف مرفق مع رسالة من شخص مجهول، حتى وإن ظهر أنه ملف نصي أو صورة لا تحمل فيروساً، لأنه يمكن التلاعب باسم الملف ليظهر الملف التنفيذي الذي يحمل فيروساً بمظهر ملف سليم يحمل صورة أو نصاً.

* لا تفتح أي ملف مرفق مع رسالة من شخص معروف إلا إذا كنت تتوقع ذلك الملف، وإذا كنت شاكاً في سلامة الملف يمكنك التحقق من صديقك بأي طريقة اتصال، وأسهلها رسالة بريدية إلكترونية استفهامية. لأنه قد يكون من أرسل الرسالة فيروس أصاب جهاز صديقك، وقام بإرسال رسائل تحتوي على برامج خبيثة باسم صديقك.

* لا تقم بفتح وقراءة أي رسالة من أشخاص مجهولين تحمل عنواناً غريباً،

مثـل : (I love you, Your money, You win). لأن بعـض بـرامج تصـفح البريـد الإلكتروني قد تقوم آلياً بتنفيذ الملفات المرفقة وعرضها مع الرسالة تلقائياً.

* عطّل ميزة تحميل الملفات المرفقة مع الرسالة الإلكترونية في برنامج البريد الإلكتروني.

* من الأفضل عدم استعراض الرسائل المعدة بواسطة لغة HTML.

* لا تحمل أي ملف من غريب، سواء عن طريق البريد الإلكتروني، أو المراسل الآني، أو مواقع مشبوهة أو غيرها من الطرق.

* افحص أي ملف تريد تحميله (سواء من إحدى وسائط التخزين، أو البريد الإلكتروني، أو المراسل الآني، أو مواقع على الإنترنت) لجهازك بواسطة برنامج مكافح الفيروسات للتحقق من خلوه من برامج خبيثة.

* استخدم برنامج مكافح الفيروسات، وحدّثه دورياً، ليتسنى للبرنامج التعرف على الفيروسات الجديدة.

* خذ نسخة احتياطية لملفاتك بشكل دوري، ولتكن خارج جهازك. قد تستفيد منها في حال تمكن أحد الفيروسات من جهازك وحذف بعض الملفات.

* تفادَ استخدام برامج المشاركة بالملفات (P2P).

* حدّث جميع برامجك (متصفح الإنترنت، متصفح البريد الإلكتروني، المراسل الآني، جدار الحماية، ونظام التشغيل(الويندوز) لتفادي الثغرات الأمنية المكتشفة بها.

* لا تثق بالغرباء على برنامج المراسل الآني، وكن حذراً مع الأصدقاء في حال تلقي أي ملف.

* لا تستغنِ عن استخدام برنامج جدار الحماية (Firewall) لسد المنافذ غير

الآمنة وتقليل الأخطار على جهازك.

في حال تلقي بلاغ عن وجود فيروس جديد، لا تقم بإرساله لأحد حتى تتأكد من أن البلاغ صحيح. يجب على المستخدم عدم إرسال بلاغات عن فيروسات، لأن ذلك من عمل مديري الأنظمة والمختصين، و لتفادي انتشار البلاغات الكاذبة.

الفيروســـات وأشـــــباهها

Viruses, Worms, Hoax

يمكننا القول إنه لا يوجد أحد لم يسمع بالفيروسات الحاسوبية بل يمكننا أيضاً أن نقول إن القليل من يسلم منها. فعند إجراء مسح لعدد كبير من الشركات لعام 2000م، وجد أن 99،67٪ منهم قد تعرضوا على الأقل لفيروس واحد[1]. ويتراوح عدد الفيروسات الجديدة كل يوم ما بين 10-20 فيروساً جديداً. بل إن شـــــركة F-Secure[2] المتخصصة في مكافحة الفيروسات أضافت 1418 تعريفاً لفيروسات جديدة خلال شهر نوفمبر لعام 2004م. ويقدر عدد الفيروسات المعروفة بقرابة 100000 فيروس. هذا عن تعدادها، فما ذاعن تكلفة أضرارها؟.

تقدر تكلفة ضرر الفيروسات لكل شركة بما يتراوح بين 100000 ومليون دولار أمريكي لكل شركة[3]. وقد قدرت تكلفة أضرار الفيروسات عالمياً لعام 2003م بـ 55 بليون دولار أمريكي وبما يتراوح بين 22-30 بليون دولار أمريكي لعام 2002م، و بـ 13 بليون دولار أمريكي لعام 2001م[4]. لاحظ أننا عندما نتكلم بشكل عام عن الفيروسات، فإننا نعني الفيروسات والديدان (Worms) معاً.

---

(1) Computer Virus Prevalence Survey, 2000.

(2) F-Secure Coropration's Data Secuity Summary for 2005.

(3) Computer Security Institute, 2001.

(4) Mirco Trend Inc.

[1] أنواعها

❖ الفيروسات Viruses

هي برامج حاسوبية خبيثة مضرة بالحواسيب، وتنتقل بين الحواسيب بعدة طرق، وتتكاثر بالاعتماد على ملفات أخرى. وهناك أنواع للفيروسات، منها ما يبدأ عمله بوقت أو حادثة معينة، حتى أصبح هناك تقويم للفيروسات التي ستعمل في يوم ما(1)، ومنها ما يكون مكوناً من أجزاء متعددة، ومنها ما تتغير صفاته بشكل دوري. ومنها ما يكون متخفياً حتى عن برامج مكافح الفيروسات.

❖ الديدان Worms

هي برامج حاسوبية خبيثة ومضرة، وتنتقل بين الحواسيب بعدة طرق، وتمتاز عن الفيروسات باعتماديتها على نفسها لتتكاثر وبسرعة الانتقال وصغر الحجم. والديدان لا تقوم عادة بعمل ضار مباشرة، كحذف البيانات، ولكن سرعة تكاثرها وانتقالها السريعان يؤثران سلباً في فعالية الحاسوب وشبكة المعلومات.

❖ الخداع أو البلاغ الكاذب Hoax

البلاغ الكاذب عن ظهور فيروس، يربك به الناس ويضيع به أوقاتهم، وقد يؤثر في الحاسوب. وهو يبدأ من شخص يريد الضرر وينتشر بواسطة أناس صدّقوا الكذبة ونشروا الخبر بغرض المساعدة في التصدي للفيروس أو الدودة. قد تأتيك رسالة بريدية كاذبة تحذرك من فيروس معين قد انتشر مؤخراً، ثم يقدم لك خطوات لمعرفة ما إذا كان جهازك قد أصيب به أم لا. وطبعاً سيكون جهازك مصاباً به لأن الخطوات لاكتشاف الفيروس تدل على أن كل جهاز صحيح مصاب لكي

---

(1) http://us.mcafee.com/virusInfo/default.asp?id=calendar.

يأكل الطعم، ثم يُطلب منك حذف بعض الملفات الأساسية للحماية من الفيروس أو الدودة، وبعد ذلك يتعطل جهازك. هذا مجرد مثال، ولمزيد من أنواع البلاغات الكاذبة يمكنك الرجوع لموقع شركة F-Secure[1].

[2] آثارها

الفيروسات بريمجات خبيثة بطبيعتها؛ فهي تؤثر تأثيراً سلبياً في الحواسيب بشكل مباشر، وفي غير الحواسيب بشكل غير مباشر. فالفيروس عندما يحذف ملفات مهمة للعملاء فإن التأثير يتعدى الحاسوب إلى العملاء وسمعة الشركة. والفيروسات لها تأثيرات شتى، منها: ما يقوم بحذف ملفات أو برامج أو تعطيلها عن العمل، ومنها ما يقوم بزراعة برامج خبيثة أخرى قد تكون تجسسية، ومنها ما يعطل الجهاز بالكلية وغيرها من الآثار الضارة.

وكذلك الديدان لها تأثيرات ضارة. كما هو معروف فإن كل برنامج يعمل في جهازك يأخذ من وقت المعالج، ومساحة في الذاكرة والقرص الصلب، حتى وإن كان البرنامج صغير الحجم، فما بالك إذا كان هناك عدد كبير من البرامج. كذلك عند انتقال ملايين البريمجات الصغيرة عن طريق الشبكة، فإنها تزحم الشبكة وتعطل منافع كثيرة معتمدة على الشبكة، أحد الأمثلة على الديدان المشهورة هو سلامر Slammer، الذي تميز بسرعة انتشار هائلة، ما مكنه من المرور على جميع عناوين الإنترنت IP البالغ عددها 4 بلايين عنوان في غضون 15دقيقة. وأدى انتشار الديدان الواسع إلى إضعاف سرعة النقل على الإنترنت، وأدى إلى تعطيل إحدى أكبر شبكات الصراف الآلي في العالم خلال فترة نهاية الأسبوع، وأبطأ أنظمة التحكم الجوي في كثير من المطارات الدولية. والأدهى من ذلك أنه استطاع أن ينفذ إلى الشبكة الداخلية لمحطة

---

(1) http://f-secure.com/virus-info/hoax/) .

الطاقة النووية في ولاية أهايو في أمريكا، وعَطَّل الحاسوب المسؤول عن مراقبة حالة المفاعل النووي للمحطة. إنه حتى مع صغر حجم هذه الديدان فإنها استطاعت أن تؤثر في حياتنا اليومية. فهذا بلاستر Blaster – نوع من أنواع الديدان– استطاع أن يؤثر في الأنظمة البنكية حول العالم، وأجبر بعض خطوط الطيران والقطارات على إلغاء بعض رحلاتها.

[3] طرق العلاج

يعتمد نوع العلاج على نوع الإصابة وتأثير الفيروس. إذا وصل ضرر الفيروس إلى حذف أغلب الملفات، أو عطّل الجهاز فما لديك سوى إعادة تثبيت جميع البرامج والملفات من النسخة الاحتياطية لملفاتك التي أوصينا بالاحتفاظ بها في طرق الوقاية. أما إذا كان ضرر الفيروس أقل من ذلك فإن برنامج مكافح الفيروسات سيساعدك على إصلاح الملفات المعطوبة قدر الإمكان، وحذف الفيروس من الجهاز. ولا تنس أن تحدّث برنامج مكافح الفيروسات ليتمكن من التعرف على الفيروس إن كان من الفيروسات الجديدة.

[4] برامج علاجية

هناك عديد من برامج مكافحة الفيروسات بأنواع ومميزات مختلفة، منها ما هو مجاني، ومنها ما هو بثمن. وهناك أيضا برامج تعمل على جهازك، ومنها ما يقوم بتفحص ملفاتك وهو على الإنترنت. ومن الأمثلة على تلك البرامج:

أ– البرامج التجارية

McAffe	http://www.mcafee.com
Symantec	http://www.symantec.com
F-SECURE	http://www.f-secure.com
Mirco Trend	http://www.trendmicro.com.

ب– البرامج المجانية

AVG Antivirus	http://free.grisoft.com

جـ – مواقع الفحص عن الفيروسات من على الإنترنت

Mirco Trend	http://housecall.trendmicro.com/housecall/start_corp.asp
RAV Antivirus	http://www.ravantivirus.com/scan/
McAffe	http://us.mcafee.com/root/mfs/
Mirco Trend	http://www.trendmicro.com/

[5] الاستخدام الأمثل لبرامج العلاج

للاستفادة القصوى من برامج مكافحة الفيروسات اتبع الخطوات التالية :

* تأكد دائماً من وجود وعمل برنامج مكافحة الفيروسات على جهازك.

* تأكد من عمل خاصية المراقبة المباشرة – إن وجدت – لكشف الفيروسات حال ولوجها الجهاز.

* تأكد من عمل خاصية مراقبة الرسائل البريدية – إن وجدت- حال تحميلها من جهاز الخادم لكشف وإزالتها الفيروسات قبل تصفح البريد.

* تأكد من تحديث برنامج مكافحة الفيروسات دورياً لكشف الفيروسات الجديدة.

* جدول برنامج المكافحة لتمشيط ملفاتك دورياً وآليا في الأوقات التي لا تعمل بها.

* استخدم جميع الخصائص التي قد تكون في نسخة برنامج المكافحة الذي لديك ، مثل : مراقبة برنامج المراسل الآني لكشف تنزيل أي فيروس حال تنزيل ملفات عبر المراسل.

الأحصنة الطروادية
Trojan Horses

يرجع الاسم إلى أسطورة قديمة مفادها أن جيش إحدى مدن الإغريق أهدى أعداءهم حصاناً خشبياً كبيراً، وعندما قبله العدو وجاؤوا به إلى بلدتهم، وفي الليل فتح الحصان فخرج منه جنود استطاعوا السيطرة على البلدة.

وحديثنا هنا عن برنامج حاسوبي يضمر أعمالاً خبيثة ومضرة، خلاف ما يظهره من أعمال مفيدة، وهو لا يتكاثر مثل الفيروسات والديدان، ولكن يكمن في النظام بشكل خفي، يحاول استغلال حاسوبك لشن الهجوم على حواسيب أخرى، أو التجسس من خلال الاحتفاظ بجميع ما أدخلت عن طريق لوحة المفاتيح، والتي قد تحتوي على رقم بطاقة الائتمان، أو كلمة المرور.

[1] أنواعها

الوصول عن بعد: هذه البرامج تسمح للمهاجم بأن يتحكم في جهازك عن بعد بشكل مخفي. من أمثلته : Back Orifice, Netbus.

مرسل البيانات Data Sender: هذا البرنامج يرسل بيانات خاصة بالمستخدم للمهاجم دون علم المستخدم. قد يرسل رقم بطاقات الائتمان، كلمة المرور، محادثاتك المكتوبة وغيرها من البيانات المهمة. يرسل البيانات بواسطة رسالة بريدية، أو تزويدها لموقع المهاجم مباشرة.

معطل الخدمات Denial of service: يعمل هذا البرنامج بالتنسيق مع نُسخ أخرى مشابهة على أجهزة أخرى مهاجمة على مهاجمة حاسوب معين وإغراق شبكته وشلّها.

وسيط Proxy : يُسخر الحاسوب المهاجم وسيطاً يستطيع المهاجم استخدامه

للوصول المتخفّي للإنترنت، بحيث لو عمل عملاً غير شرعي وتمت متابعة العملية فإن الحاسوب الذي جرى تسخيره هو آخر نقطة يمكن تتبع العملية إليها.

معطل البرامج Blocker : يقوم هذا البرنامج، بتعطيل بعض البرامج، خاصة الحساسة، مثل: برامج مكافحة الفيروسات، وبرامج جدران الحماية ليجرد جهازك من أي حماية ضد الهجمات المستقبلية.

[2] طريقة عملها

يقوم المهاجم بزرع برنامج مستقبل أو خادم (Client/ Server) (لاستقبال الأوامر والتعليمات) على جهاز الضحية بعدة طرق ذكرناها سابقاً، ويفتح منفذاً خاصاً به للاتصال عن طريق الإنترنت، ثم يقوم البرنامج بإرسال عنوان جهازك على الإنترنت (IP) للمهاجم، بعد ذلك يقوم المهاجم بالاتصال بذلك البرنامج ليبدأ التحكم بجهاز الضحية.

[3] برامج علاجية

بما أن هناك برنامجاً خبيثاً و منفذاً مفتوحاً للاتصال فإن الحل الأنجع للعلاج من الأحصنة الطروادية يكمن في نوعين من البرامج هما:

* **برنامج جدار الحماية (Firewall)**: للتحكم في المنافذ ومراقبتها، ومنع المنافذ غير الشرعية من الاتصال بالإنترنت، وبالتالي قطع الصلة بالمهاجم. وهذا العمل مهم، لكن لا يفيد في حال اتخذ البرنامج الخبيث قناة أخرى شرعية للاتصال، كأن يستخدم البريد الإلكتروني، أو المراسل الآني. و يمكن للقارئ معرفة المزيد عن برامج جدار الحماية في الجزء الخاص بها في هذا الكتاب.

* **برنامج لصيد البرامج الخبيثة بشكل عام والأحصنة الطروادية بشكل خاص ومكافحتها**: إن برامج مكافحة الفيروسات تصيد جزءاً من الأحصنة الطروادية، لكن ليس

جميعها، لذا يلزمك برامج مكافحة خاصة بالأحصنة الطروادية لحماية جهازك بشكل أفضل، ولا تنس أن تحدّث برامج المكافحة بشكل دوري لصيد البرامج الخبيثة الجديدة. ومن برامج مكافحة الأحصنة الطروادية:

lockdown2000	http://www.lockdown2000.com
Pest Patrol	http://www.safersite.com
The Cleaner	http://www.moosoft.com
Tuscan	http://agnitum.com/products/tauscan/
Trojan hunter	http://www.trojanhunter.com/
Trojan remover	http://www.simplysup.com/

لا تنس بعد اكتشاف أي حصان طروادي ومكافحته أن تقوم بالتالي:

- استبدل كلمات المرور المسجلة على الجهاز والتي يمكن أن تكون قد سُرقت من قبل المهاجم عن طريق الحصان الطروادي.
- تفحص جهازك باستخدام برنامج مكافحة الفيروسات، تحسباً من أن يكون المهاجم قد زرع فيروساً في جهازك.

رسائل الاصطياد الخادعة
Phishing Scam

كثرت في الآونة الأخيرة طرق الاحتيال والخداع حتى أصبحت أكثر تفنناً وإتقاناً. ومن الطرق المستحدثة ما يسمى رسائل الاصطياد الخادعة، وهي رسائل تبدو بالشكل والعنوان البريدي أنها مرسلة من منظمة حقيقية (وغالباً ما تكون المنظمة بنكاً)، وتفيد بأن هناك تحديثاً للبيانات، أو إجراءات جديدة للحماية والأمن وتطلب منك الدخول لموقع البنك عن طريق الرابط المزود مع الرسالة. وعند الانتقال للموقع الوهمي، الذي يبدو بشكله وتصميمه، وكذلك عنوانه كالبنك المعني، يطلب منك بيانات خاصة، ككلمة المرور، أو معلومات بطاقة الائتمان، ثم بعد الحصول على تلك المعلومات الثمينة يحيلك لموقع البنك الحقيقي.

هناك نمو مطرد يصل إلى 36٪ شهرياً في عدد الرسائل الجديدة من هذا النوع، لقد بلغت وقد بلغ عدد رسائل الاصطياد الخادعة 6597 رسالة مختلفة في شهر أكتوبر لعام 2004م.

لنأخذ مثالاً واقعياً على هذه الطريقة سجلته مجموعة مكافحة رسائل الاصطياد[1].

لنفرض أنك أحد عملاء بنك يدعى SunTrust Bank ؛ وجاءتك رسالة نصها:

---

(1) http://www.antiphishing.org/.

Dear SunTrust Bank Customer,

To provide our customers the most effective and secure online access to their accounts, we are continually upgrading our online services. As we add new features and enhancements to our service, there are certain browser versions, which will not support these system upgrades. As many customers already know, Microsoft Internet Explorer has significant 'holes' or vulnerabilities that virus creators can easily take advantage of.

In order to further protect your account, we have introduced some new important security standards and browser requirements. SunTrust security systems require that you test your browser now to see if it meets the requirements for SunTrust Internet Banking.

Please sign on to Internet Banking in order to verify security update installation. This security update will be effective immediately. In the meantime, some of the Internet Banking services may not be available.

SunTrust Internet Banking

الشكل رقم (10): رسالة اصطياد

فحوى الرسالة أن البنك قام بتعزيز أنظمة الحماية وتحديث خدماته البنكية الشبكية، ويريد منك التأكد من أن برنامج متصفح الإنترنت الذي تعمل عليه متوافق مع التحديثات الجديدة، لذا يلزمك الدخول لموقع البنك والتسجيل بواسطة الضغط على الرابط المعطى. وعند الضغط على الرابط يحولك إلى موقع البنك المزيف كما هو موضح بالشكل (11).



الشكل رقم (11): موقع البنك المزيف.

الموقع يبدو حقيقياً لسببين قد يصدقهما المستخدم:

أولاً: التصميم قريب جداً للموقع الحقيقي.

ثانياً: العنوان (URL) يبدو حقيقياً وهو:

(http://internetbanking.suntrust.com).

لقد تحايلوا بتغطية شريط العنوان بشريط آخر معمول بلغة جافا. ويمكن معرفته بالضغط بالزر الأيمن للفأرة على شريط الأدوات، ثم اختيار خصائص، ثم تمريره على شريط العنوان ليتضح أن شريط العنوان مغطى كما هو موضح في الشكل. شريط العنوان الحقيقي يشير إلى الموقع المزيف بعنوان: (http://82.90.165.65/s/login.html). طبعاً بعد أخذ معلوماتك السرية يخبرك بأن برنامج المتصفح متوافق مع الخدمات الجديدة، ثم يحيلك إلى موقع البنك الحقيقي، وكأن شيئاً لم يكن، حتى لا يثير شكك! وإذا كنت من عملاء البنك وتستخدم الخدمات النسيجية للبنك وجاءتك مثل تلك الرسالة فإنك قد تصدّقهم، خاصة أنه طلب منك المعلومات عن طريق موقعهم، والذي يبدو حقيقياً.

[1] طرق الوقاية

* كن حذراً من الرسائل التي تطلب بشكل مستعجل معلومات شخصية سرية.

* رسائل الخداع موجهة للعموم؛ أما الرسائل المرسلة من الجهات الحقيقية فتكون مخصوصة باسمك.

* لا تستخدم الرابط، بل قم بمحادثة الجهة مباشرة، أو اكتب بنفسك موقع الجهة في شريط العنوان على برنامج متصفح الإنترنت مباشرة.

* لا تقم بتعبئة أي نموذج بالبريد الإلكتروني. تعبئة بياناتك لابد أن تكون عن

طريق موقع ومحمي بالتأكد من أن العنوان يبدأ بـ https وليس http فقط ، وشكل القفل التالي في زاوية المتصفح السفلى.

* حدّث برنامج المتصفح و نظام التشغيل بأحدث الترقيات الأمنية.

لكن إذا أكلت الطعم وقدّمت بيانات سريه فعليك الإبلاغ في أسرع وقت ممكن للجهة الحقيقة لإلغاء البطاقة واستبدال بطاقة ورقم جديدين بها ، أو تغيير رقم الحساب ، أو كلمة المرور ، أو اسم المستخدم ، أو غيرها من الإجراءات اللازمة لتلافي أي خسائر.

لا تعد المراسلات الإلكترونية وثائق رسمية لدى المؤسسات المالية مثل البنوك ، لذا ينصح الحذر من الرسائل الإلكترونية المرسلة من قبل البنوك و التي تطلب معلومات سرية ، فقد تكون تلك الرسائل غير صحيحة المصدر.

البرامج التجسسية و أشباهها
Spyware

البرامج التجسسية هي كل برنامج يراقب سلوكك على جهازك من مراقبة كتاباتك إلى مراقبة المواقع التي تزورها. والهدف من برامج التجسس يكاد ينحصر في أمرين: أولهما: التجسس الخبيث لاستسقاء معلومات سرية، مثل كلمات المرور، وأرقام الحسابات البنكية، و والآخر: لأغراض تجارية، مثل: معرفة أنماط المستخدم الاستهلاكية، أو محركات البحث الأكثر استخداماً، أو المواقع التجارية الأكثر تسوقاً.

إن تلك البرامج تستنزف طاقات الجهاز والاتصال دون إذن واضح منك. وكما تعلم أن مجرد المراقبة، وتسجيل السلوك أو المعلومات يتطلب وقتاً من المعالج، ومساحة من الذاكرة، ووحدة التخزين الدائمة، وجزءاً من كمية البيانات المرسلة عن طريق وسيط الاتصال.

[1] أنواعها

*** برنامج متابعة تصرفات المستخدم أو التجسس البسيط Spyware**

هي كل برنامج يتجسس على سلوك المستخدم أو معلوماته بعلم، أو بدون علم.

*** برنامج تسجيل نقرات لوحة المفاتيح Keystroke Logger**

تخيل أن كل ما تكتبه على لوحة المفاتيح يُسّجل وقد يُرسل لغيرك. نعم كل شيء، من رسائل بريدية إلكترونية، ودردشة، إلى كلمات المرور، وأرقام بطاقاتك البنكية. هناك برامج وقطع إلكترونية لعمل ذلك، وهي تُسَوق على أنها برامج مراقبة لأب على أبنائه أو لزوج على زوجته، أو العكس. لكن في الوقت نفسه تُستخدم تلك البرامج استخداماً خبيثاً، كأن تُزرع تلك البرامج في جهازك - من غير علمك - بواسطة أحد مهاجمي

جهازك، ويتلقى ما تكتبه بشكل مستمر. وبرنامج تسجيل نقرات لوحة المفاتيح هو نوع من أنواع برامج التجسس Spyware، والأحصنة الطروادية.

* **برامج الإعلانات Adware**

هي برامج أو بريمجات هدفها التسويق التجاري بطريقة إجبارية غير مرغوبة. ومن الأمثلة على تلك البرامج:

(1) تقديم إعلانات لمنتجات معيّنة بمجرد البحث، عن مثيلاتها في محرك البحث.

(2) تعطيل محرك البحث وتقديم محرك بحث آخر مقلد ليخدم مهام الجهة الإعلامية لبرنامج الإعلانات.

(3) تحويل المستخدم إلى مواقع تجارية دون إذنه.

* **الصفحات الفقّاعية أو الانبثاقية Popup**

هي برامج فقّاعية أو انبثاقية تخرج بين الفينة والأخرى، كإعلانات أثناء تصفح الإنترنت، وتستهلك موارد النظام والاتصال، خاصة إذا كان الاتصال بسرعة 56 كيلوبت/ثانية. وقد تؤدي البرامج الفقاعية إلى مشاكل أمنية جرّاء الإخفاق في سد الثغرات الأمنية للحاسوب.

[2] طرق الإصابة بها

تتمكن تلك البرامج من النزول في حاسوبك باستخدام إحدى طريقتين:

أولاهما: عن طريق وجودها مع البرامج المجانية أو المشبوهة.

والأخرى: عن طريق استغلال إحدى الثغرات الأمنية في جهازك للوصول إليه.

[3] طرق معرفة الإصابة بها

هناك عدة طرق للتعرف على الإصابة ببرامج التجسس والمراقبة، من أوضحها:

* كثرة الصفحات الانبثاقية التي ليس لها صلة بالموقع المزار، مثل صفحات بصور إباحية.

* حاسوبك يحاول الاتصال بالهاتف دون أمرك. وهناك برامج تقوم بالاتصال عن طريق هاتفك ودون أمرك وعلمك بأرقام هواتف دولية باهظة التكلفة.

* يصبح حاسوبك بطيء الاستجابة لدرجة ملحوظة.

* عندما تقوم بالبحث فإن المتصفح يستخدم محركاً للبحث غير الذي حددته.

* قائمة المواقع المفضلة في برنامج متصفح الإنترنت يحتوي على مواقع لم تقم بإضافتها.

* صفحة البداية تشير إلى موقع لم تقم باختياره كصفحة بداية، ويبقى كذلك حتى لو غيرت صفحة البداية.

[4] طرق الوقاية

هناك عدة طرق وقائية ضد برامج التجسس وغيرها من البرامج الضارة:

* داوم على سد الثغرات الأمنية بمتابعة آخر التحديثات لبرامجك الحساسة مثل: نظام التشغيل، ومتصفح الإنترنت، وبرنامج البريد الإلكتروني.

* دعّم حاسوبك ببرنامج أو جهاز جدار الحماية لتقليل تعرّضه للاختراق من قبل الغير.

* دعّم حاسوبك ببرنامج مكافح الفيروسات.

* عند الحاجة لبرامج مجانية حمّلها من مواقع معروفة مثل www.download.com.

* اقرأ محتويات الاتفاقية الخاصة باستخدام البرامج، لأن بعضها تنص بوضوح على أن البرنامج سيقوم بمراقبة سلوكك وإرسال بيانات لجهة خارجية.

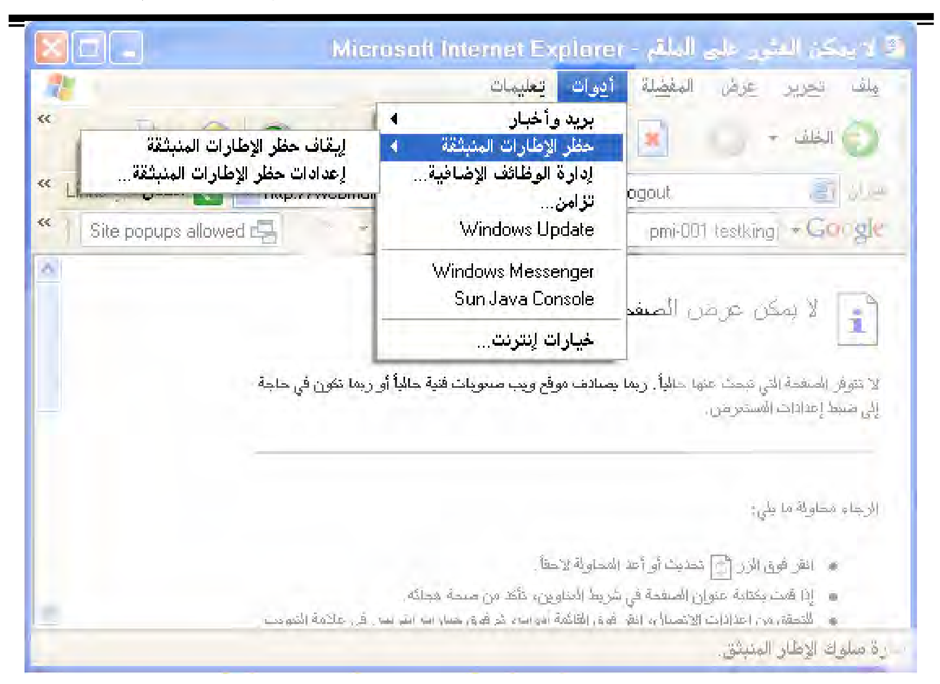
* تحاش زيارة المواقع المشبوهة مثل المواقع الإباحية، و مواقع القرصنة.

* تحاش برامج المشاركة P2P.

* تأكد من مرفقات رسائل البريد الإلكتروني، ولا تقم بفتحها حتى تتأكد من خلوها من الفيروسات، وأنها مرسلة من شخص موثوق به ومعروف، ومتوقعة الوصول.

* تفحص حاسوبك بشكل دوري باستخدام برنامج مكافحة الفيروسات، وبرنامج مكافحة برامج التجسس.

* دعّم حاسوبك ببرنامج لمكافحة برامج التجسس، والصفحات الفقاعية. وإذا كان حاسوبك مزوداً بالتحديث الجديد لنظام الويندوز اكس بي SP2 فيمكنك استخدام خاصية إيقاف الرسائل الفقاعية، ويمكن تفعيلها من برنامج متصفح الإنترنت تحت قائمة "أدوات"، كما في الشكل رقم (12).



الشكل رقم (12): خاصية إيقاف الرسائل الفقاعية

* تأكد من أن نهاية سلك لوحة المفاتيح موصول بشكل مباشر للحاسوب ولا توجد قطعة بينهما.



الشكل رقم (13): وصل لوحة المفاتيح بالحاسوب.

* تأكد من أن مستوى الأمان في برنامج متصفح الإنترنت مرتفع كما في الشكل

التالي رقم (14).



الشكل رقم (**14**): مستوى الأمان في برنامج متصفح الإنترنت.

[5] برامج علاجية

هناك برامج عديدة لمكافحة برامج التجسس، منها على سبيل المثال:

Ad-Aware Pro.	http://www.lavasoft.de
Destroy & **Search** - **Spybot**	http://www.safer-networking.org/en/index.html
Pest Patrol	http://www.pestpatrol.com/

الخلاصة

البرامج الخبيثة هي برامج يكون كل مهامها أو أحدهما عمل إفسادي،

كالتجسس أو التخريب ، أو استنزاف الموارد الحاسوبية. و تنتقل هذه البرامج إلى الحاسوب ، أو شبكة المعلومات بوسائل متعددة و ملتوية ترتكز في معظمها على استدراج المستخدم. وينبغي أن يتفطن المستخدم لهذه الطرق ؛ كما ينبغي أن يتبع الأساليب التي ثبت نجاحها لمنع الإصابة بالبرامج الخبيثة ابتداء ، أو التعامل الصحيح معها في حال وصولها إلى شبكة المعلومات.

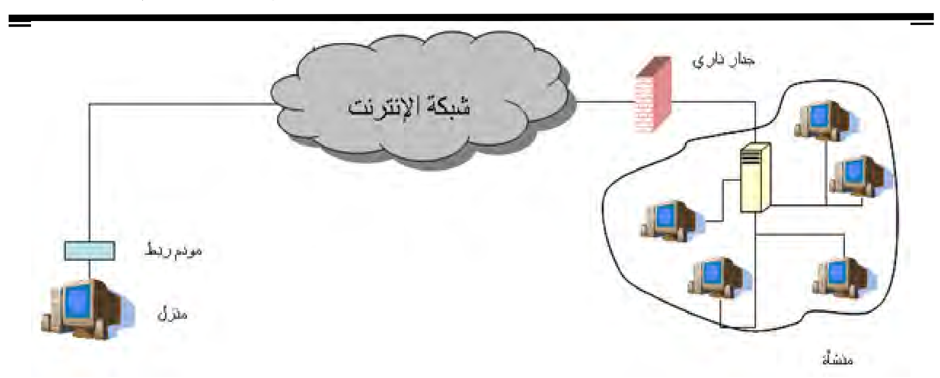
جدران الحماية
Firewall

إن الفوائد والخدمات التي جاءت بها شبكة الإنترنت لم تأت خلواً من المنغصات، فراجت سوق الطفيليين (Hackers) الذين لا هم لهم سوى التلصص على معلومات الآخرين. كما ظهر أناس يستمتعون بإلحاق الأذى بالآخرين، إما بحذف وثائقهم المهمة، أو العبث بمحتوياتها، أو نشر البرامج السيئة (Malware) مثل الديدان، والفيروسات، وأحصنة طروادة وغيرها.

ولمقاومة تلك الأخطار والحد منها ظهرت تقنيات ومفاهيم متعددة، من أكثرها انتشاراً جدران الحماية (Firewalls) التي تسمى أيضا الجدران النارية. ولتقريب المعنى للأذهان نقول إن جدار الحماية نظام مؤلف من برنامج (software) يجري في حاسوب، وهذا الحاسوب قد يكون حاسوبا عاديا، مثل الحاسوبات الشخصية، أو حاسوبا بني بمواصفات خاصة ليكون أكثر قدرة على تلبية المتطلبات الفنية الخاصة بجدار الحماية. وفكرة جدار الحماية تشبه فكرة نقطة التفتيش التي تسمح بمرور أناس، وتمنع مرور آخرين، بناء على تعليمات مسبقة.

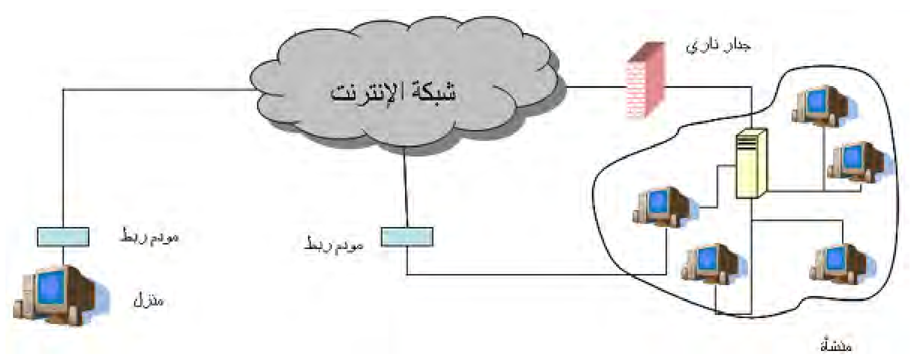
[1] وضع جدار الحماية

ولتوفير بعض الحماية لنفسها تقوم المنشآت بوضع جدار حماية لعزل شبكتها الداخلية عن شبكة الإنترنت، كما يوضح الشكل (15). بيد أن هذا العزل لا يمكن أن يكون كلياً؛ وذلك للسماح للجمهور بالاستفادة من الخدمات المقدمة، وفي الوقت ذاته منع الطفيليين والمخربين من الدخول، وتتاح من خلال البرنامج الموجود في جدار



الشكل رقم (15) : وضع جدار الحماية.

الحماية مراقبة المعلومات بين الشبكة الداخلية للمنشأة والعالم الخارجي. ولتحقق الغاية من جدار الحماية فإنه لا بد من وضعه في موقع استراتيجي يضمن ألا تخرج المعلومات أو تدخل إلى الشبكة الداخلية إلا عن طريقه. ولذلك فإن الوضع الموضح في الشكل رقم **(16)**غير مقبول عند المختصين في مجال أمن المعلومات ؛ لأن الوصول للشبكة الداخلية ممكن عن طريق الاتصال بجهاز المودم الذي يشكل في هذه الحالة بوابة خلفية يلج المتطفلون والمخربون عبرها.



الشكل رقم (16): وضع غير محبذ لاستخدام جدار الحماية

[2] كيف تعمل جدران الحماية؟

طريقة عمل جدران الحماية يحددها تصميم جدران الحماية. لتبسيط هذا الموضوع نقول إن هناك ثلاثة أساليب في تصميم جدار الحماية هي :

(أ) أسلوب غربلة مظاريف البيانات المرسلة (Packet Filtering)

تنتقل المعلومات على شبكة الإنترنت في صورة مظروف إلكتروني. وإذا كان جدار الحماية مصمما بهذه الطريقة فإنه يفحص كل مظروف يمر عبره، ويتحقق من تلبية المظروف لشروط معينة يحددها الشخص الذي يدير جدار الحماية، وهذه الشروط تدخل بطريقة خاصة في البرنامج المكون للجدار الناري.

(ب) أسلوب غربلة المظاريف مع تغيير عناوين المظاريف القادمة من الشبكة الداخلية (أي المظاريف الصادرة)

عندما يقوم مستخدم حاسوب ما بالتعامل مع شبكة الإنترنت، مثل أن يتصفح موقعا ما، أو يرسل بريداً إلكترونياً فإن هناك أمورا كثيرة تدور خلف الكواليس دون أن يشعر بها المستخدم. ومن ذلك أن نظام التشغيل الموجود في الحاسوب يقوم بإرسال بيانات إلى شبكة الإنترنت لتحقيق رغبة المستخدم، سواء كانت تصفح موقع، أو إرسال بريد. وهذه البيانات يجمعها الجهاز في مظاريف إلكترونية تحمل –ضمن ما تحمل من معلومات– العنوان الرقمي المميز للحاسوب الذي أرسلها، أو ما يسمى (IP Address). وهذا العنوان يميز هذا الجهاز عن سائر الأجهزة المرتبطة في شبكة الإنترنت، كما سنوضح في موضع آخر من الكتاب. وفائدة هذا العنوان هي تمكين الأطراف الأخرى من إرسال الردود المناسبة للحاسوب الذي أرسل البيانات، وبالتالي تقديم الخدمة للمستخدم الذي طلبها. لكن هذا العنوان قد يُستخدم من قبل أصحاب المآرب السيئة لشن هجمات على ذلك الحاسوب.

وعند اعتماد أسلوب غربلة المظاريف مع تغيير عناوين المظاريف الصادرة يقوم

جدار الحماية بطمس العنوان المميز للحاسوب الذي أرسل المظروف من المظروف الإلكتروني، ووضع العنوان الخاص بالجدار نفسه بدلا منه. وبهذا لا يرى الأشرار المترصدون من الشبكة الداخلية سوى جدار الحماية، فيحجب الجدار كل أجهزة الشبكة المراد حمايتها، وينصب نفسه وكيلاً (Proxy) عنها. وعندما يرغب الموقع المتصفَح الرد فإنه يرسل رده في مظاريف تحمل عنوان جدار الحماية، وبهذا تأخذ كل المظاريف القادمة (الواردة) إلى الشبكة الداخلية عنوان جدار الحماية، ويقوم هو عند استلامها بغربلتها، ثم توجيهها إلى وجهتها النهائية. ولابد في هذه الحالة أن يحتفظ الجدار بجدول متابعة يربط فيه بين عناوين المظاريف الصادرة والواردة. وهذا التنظيم يوفر مقداراً أكبر من الحماية مقارنة بالطريقة الأولى؛ لأن الجدار يحجب عناوين الشبكة الداخلية، مما يصعب مهمة من أراد مهاجمتها. وهذه التقنية تعرف باسم تحويل العناوين الرقمية (Network Address Translation)، أو (NAT) اختصارا، و سنتناولها بشيء من التفصيل في موضع آخر.

(جـ) أسلوب مراقبة السياق (Stateful Inspection)

هنا يقوم جدار الحماية بمراقبة حقول معينة في المظروف الإلكتروني، ويقارنها بالحقول المناظرة لها في المظاريف الأخرى التي في السياق نفسه، ونعني بالسياق هنا مجموعة المظاريف الإلكترونية المتبادلة عبر شبكة الإنترنت بين جهازين لتنفيذ عملية ما. وتجري غربلة المظاريف التي تنتمي لسياق معين إذا لم تلتزم بقواعده؛ لأن هذا دليل على أنها زرعت في السياق وليست جزءاً منه، مما يولد غلبة ظن بأنها برامج مسيئة، أو مظاريف أرسلها شخص متطفل .

وهناك عدة معايير يمكن استخدام واحد منها أو أكثر لتمييز صحيح المظاريف

من سقيمها ، ومن هذه المعايير ما يلي :

أ- العنـــوان الرقمـــي (IP Address): وهــو - كما أشرنا سابقا - رقم يميز كل جهاز مشترك في شبكة الإنترنت ، فيمكن للجدار الناري أن يجيز مرور مظروف ما ، أو يمنعه بناء على العنوان الرقمي للمرسل أو المستقبل.

ب- اسم النطاق (Domain Name) : ليسهل على المستخدم العادي الوصول إلى المواقع على شبكة الإنترنت فإن المواقع تعطى أسماء ذات معنى ، إضافة إلى العناوين الرقمية المذكورة سابقاً. فمثلاً اسم النطاق (www.ksu.edu.sa) يدل على موقع جامعة الملك سعود على شبكة الإنترنت ، بينما يدل (www.moe.gov.sa) على موقع وزارة التربية والتعليم في المملكة العربية السعودية. وتمكن برمجة جدار الحماية بحيث يمنع مرور المظاريف الإلكترونية القادمة من نطاق (Domain) معين.

(جـ) بروتوكول التخاطب المستخدم: المقصود بالبروتوكول هنا الطريقة المعينة للتخاطب وتبادل المعلومات بين طالب الخدمة والجهة التي تقدم تلك الخدمة. وطالب الخدمة هنا قد يكون إنساناً ، أو برنامجاً مثل المتصفح (Browser). وبسبب تنوع الخدمات التي تقدم في شبكة الإنترنت ، فإن الشبكة تعج بالبروتوكولات اللازمة لتسهيل تقديم تلك الخدمات لمن يريدها ، ومن هذه البرتوكولات :

(1) بروتوكـــول (HTTP): يستخدم لتبادل المعلومات بين برنامج المتصفح ومزود الخدمة في الموقع الذي يزوره المتصفح.

(2) بروتوكول (FTP): يستخدم لنقل الملفات خاصة كبيرة الحجم منها ، بدلاً من إرسالها كمرفقات (Attachments) في البريد الإلكتروني .

(3) بروتوكول (SMTP): يستخدم لنقل البريد الإلكتروني.

(4) بروتوكول (SNMP): يستخدم لإدارة الشبكات ، وجمع المعلومات عن بعد.

(5) **بروتوكول (Telnet)**: يستخدم للدخول على جهاز ما من بعد، وتنفيذ بعض الأوامر داخله.

وهنا نقول إن الشخص المسؤول عن جدار الحماية يمكنه برمجة جدار الحماية بحيث يغربل المظاريف بناء على البروتوكول المستخدم لتراسل البيانات، وهناك خانة في المظروف تدل على نوع البروتوكول، فيقوم جدار الحماية بمعاينتها، فإن وجد أن البروتوكول مسموح به فإن جدار الحماية يسمح للمظروف بالمرور، وإلا فإنه يحذف المظروف.

وهناك معايير أخرى يمكن استخدامها أساساً للغربلة، مثل رقم المنفذ الذي سيستقبل المظروف في الجهاز المرسل إليه. كما يمكن برمجة بعض جدران الحماية للبحث عن كلمات أو عبارات معينة في المظاريف، فتحذف منها ما يحتوي على تلك العبارات وتمرر الباقي.

[3] أنواع جدران الحماية

يمكن تصنيف جدران الحماية من حيث الجهة المستفيدة منها إلى ما يلي:

(أ) **جدران نارية لحماية المنشآت الكبيرة (Enterprise)**: وهذا النوع توفره شركات كبرى متخصصة مثل (CISCO) و(Nortel) و(Symantec). وغالباً ما توفر الشركة المصنعة أنواعاً متعددة من جدران الحماية تتفاوت من حيث سرعتها والخدمات التي تقدمها. وهذا النوع من جدران الحماية يتميز بما يلي:

(1) إن جدار الحماية يكون –غالبا– في جهاز قائم بذاته مصمم لغرض معالجة البيانات بسرعة فائقة، أي أنه ليس مجرد برنامج يعمل في جهاز حاسوب عادي.

(2) تعدد الخدمات التي يقدمها جدار الحماية، مثل: غربلة المظاريف، والحماية ضد الفيروسات، وحماية البريد الإلكتروني، والتشفير.

(3) تشغيل جدار الحماية يحتاج إلى مهارات فنية متقدمة.

(4) ارتفاع كلفة الشراء والتشغيل.

والشكل (17) يظهر صورة لأحد جدران الحماية التي تصنعها شركة (CISCO).



الشكل رقم (17): جدار حماية من شركة CISCO.

(ب) جدران نارية لحماية المنشآت الصغيرة: و هذا النوع يشبه سابقه في كونه جهازا مخصصا قائما بذاته، إلا أنه لا يجاريه من حيث سرعة معالجة البيانات، أو تعدد الخدمات المقدمة، ولهذا فإنه أقل سعراً. من سابقه.

(جـ) جدران نارية لحماية الأجهزة الشخصية: جدران الحماية هذه في أغلبها ما هي إلا برامج تحمل في الحاسوب الشخصي، بحيث تمر من خلالها جميع المعلومات الخارجة من الحاسوب أو الداخلة إليه. وفي هذا المجال أيضا يتنافس عدد من الشركات على السوق الكبير لجدران الحماية الشخصية. ومن أمثلة المنتجات في هذا المجال ما يلي:

(1) Norton Personal Firewall

(2) ZoneAlarm .

(3) Sygate

(4) McAfee

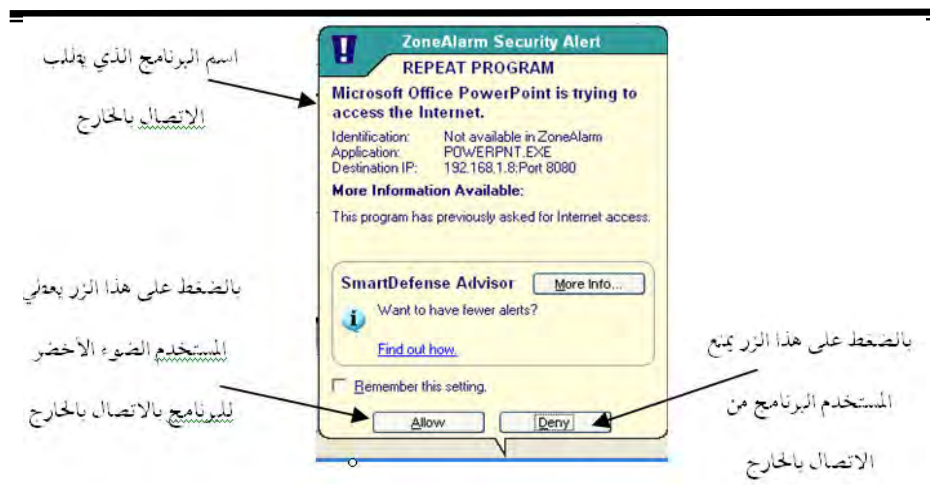
و يقدم هذا النوع من جدران الحماية عدة خدمات، مثل غربلة المظاريف، والحماية ضد الفيروسات، وحماية البريد الإلكتروني، والتشفير، والوقاية من برامج التجسس (Spyware). و يمكن تنزيل هذه البرامج من شبكة الإنترنت، إما مجاناً مثل: (ZoneAlarm)، أو بثمن مثل (ZoneAlarm Pro).

وفي الشكل (18) توضيح للشاشة الرئيسة للجدار الناري ZoneAlarm مع وصف لأهم وظائفه.

و عندما يحاول برنامج موجود داخل الحاسوب الاتصال بالخارج، كالاتصال بموقع موجود على شبكة الإنترنت، يقوم جدار الحماية (ZoneAlarm) بعرض رسالة كتلك الموضحة في الشكل رقم (19)، ويطلب من المستخدم اتخاذ القرار بشأن السماح للبرنامج بالاتصال بالخارج، أو منعه من ذلك. وبهذه الآلية يمنع جدار الحماية البرامج الخبيثة التي قد توجد في جهاز المستخدم من تسريب المعلومات المخزنة في الجهاز إلى الخارج دون علم المستخدم.



الشكل رقم (18): الشاشة الرئيسة لجدار حماية من ZoneAlarm .



الشكل رقم (19): رسالة تحذيرية من جدار الحماية.

كما أن جدار الحماية يمكن تهيئته بحيث يعرض رسالة تحذيرية في كل مرة يحاول برنامج موجود بالخارج الاتصال بالحاسوب الذي يوجد به جدار الحماية، والغرض من هذا واضح، فإنه توجد في شبكة الإنترنت برامج خبيثة كثيرة تحاول الوصول إلى الحواسيب لإتلافها، أو إتلاف البيانات التي فيها.

الخلاصة

بسبب كثرة الأخطار التي تهدد شبكات المعلومات من خارجها، نشأت فكرة إقامة جدران الحماية التي تسمى أيضا الجدران النارية، التي يمكن وصفها بأنها نظام مؤلف من برنامج (software) يعمل في حاسوب، وهذا الحاسوب قد يكون حاسوبا عاديا مثل الحاسوبات الشخصية، أو حاسوبا بني بمواصفات خاصة ليكون أكثر قدرة على تلبية المتطلبات الفنية الخاصة بجدار الحماية. وفكرة جدار الحماية تشبه فكرة نقطة التفتيش التي تسمح بمرور أناس، وتمنع مرور آخرين، بناء على تعليمات مسبقة. وتتعدد أنواع جدران الحماية بحسب حجم منظومة المعلومات المراد حمايتها والتقنية المستخدمة، و يجب تاكيد أهمية وجود جدران الحماية الشخصية بوصفها أحد خطوط الدفاع الأخيرة.

تحويل العناوين الرقمية
Network Address Translation

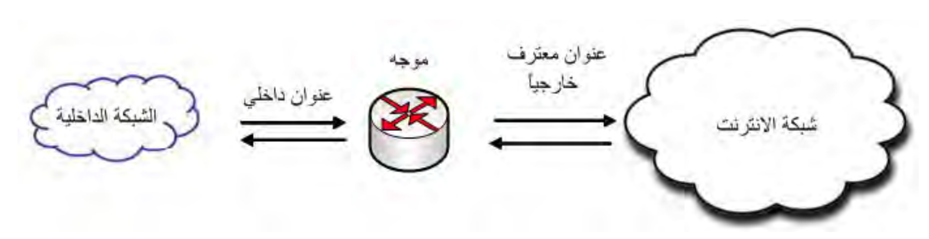
لقد فاق نمو شبكة الإنترنت كل التوقعات، ومع أن حجم شبكة الإنترنت غير معروف على وجه الدقة، فإن بعض التقديرات تشير إلى أنه يرتبط بهذه الشبكة قرابة مائة مليون من الحواسيب يستخدمها 350 مليون إنسان. والشيء المؤكد أن حجم الشبكة يتزايد كل عام. وكل جهاز يرتبط بشبكة الإنترنت يحتاج إلى عنوان رقمي يميزه عن باقي الأجهزة، وهذا يعرف باسم (IP Address)، وهذا العنوان الرقمي مكون من 32 خانة ثنائية، أي ما يكفي لإيجاد (4.294.967.296) عنواناً مميزاً. لكن العدد الحقيقي المتاح أصغر من هذا بسبب الطريقة التي تستخدم فيها العناوين الرقمية. ولمواجهة معضلة قلة العدد المتاح من العناوين الرقمية فكر المختصون في إيجاد حلول لهذه المعضلة، وكان منها أسلوب تحويل العناوين الرقمية، أو ما اصطلح على تسميته (NAT) الذي هو اختصار لمصطلح (Network Address Translation).

[1] الفكرة الأساس لتقنية (NAT)

هناك منظمة تسمى (Internet Assigned Numbers Authority IANA) تتولى إعطاء العناوين الرقمية لمن يطلبها، ولا يكون العنوان معترفاً به - وبالتالي صالحاً للاستخدام- ما لم يُصدر من تلك المنظمة التي تحرص على أن يكون العنوان الرقمي فريداً، أي أنه يدل على جهاز أو شبكة. وبسبب قلة العدد المتاح من العناوين الرقمية فإنه غالباً ما تعطى شبكة ما -ولنسمها الشبكة الداخلية - رقماً واحداً، أو عدداً من الأرقام ليكون معرفاً لها عند بقية شبكة الإنترنت. ثم تعطى الأجهزة المكونة للشبكة الداخلية عناوين رقمية لغرض الاستخدام الداخلي فقط بحيث لا يتكرر رقم واحد داخل الشبكة المعينة. غير أن هذه الأ[illegible]ر خارج الشبكة المعينة، أي أن عنوانا

رقميا داخليا ما قد يستخدم في أكثر من شبكة ، تماماً كما يتكرر رقم التحويلة الداخلية الهاتفية في أكثر من شركة، لكن يميز بينها الرقم الهاتفي الذي يعطى للمنشأة ككل.

ويأتي دور تقنية (NAT) عندما يرغب جهاز في الشبكة الداخلية الاتصال بجهاز خارج الشبكة الداخلية. ولأن العنوان الرقمي للجهاز الداخلي غير معترف به خارجياً فإننا ننصب جهازاً وسيطاً بين الشبكة الداخلية وشبكة الإنترنت، مهمته تحويل العنوان الرقمي الداخلي إلى رقم خارجي معترف به، ثم يرسل المظاريف الإلكترونية (Packets) إلى الجهاز المقصود حامله الرقم الخارجي على أنه العنوان الرقمي للجهاز المرسل الواقع داخل الشبكة المحلية. وعند عودة هذه المظاريف يبادر الجهاز الوسيط بالنظر إلى عنوان المرسل إليه الموجود فيها ويحولها نحو الجهاز الداخلي المقصود. وغالباً ما يكون الجهاز الوسيط الذي يطبق تقنية (NAT) إما جداراً نارياً (Firewall) أو موجَّها (Router).



الشكل رقم (20): عمل تقنية NAT .

[2] كيف تعمل تقنية (NAT)

هناك عدة طرق تعمل بها تقنية (NAT) ، منها :

(أ) **النمط الثابت للتحويل (Static NAT)**: يخصص الجهاز الوسيط لكل عنوان رقمي داخلي عنواناً رقمياً خارجياً ثابتاً لا يتغير.

(ب) النمـــــــط المتغير للتحـــويـــــل (Dynamic NAT): في هـذا النوع يكون لدى الجهاز الوسيط عدد محدد من العناوين الرقمية الخارجية، وكلما طلب جهاز داخلي الاتصال بشبكة الإنترنت أعطاه جهاز التحويل أياً من العناوين الرقمية الخارجية، ويقوم الجهاز الداخلي باستخدام العنوان الرقمي الخارجي عنوانا مؤقتا له للتواصل مع باقي شبكة الإنترنت، أي أنه يضع هذا العنوان المؤقت على المظاريف التي يرسلها باعتبار أنه عنوان المرسل. وعند رغبة جهاز موجود في الشبكة في الرد فإنه يستخدم هذا العنوان المؤقت باعتباره عنوان المرسل إليه. و بعد انتهاء المحادثة وقطع الجهاز اتصاله بالإنترنت، يعود العنوان المؤقت إلى الجهاز الوسيط الذي قد يمنح هذا العنوان لجهاز آخر فيما بعد، وهكذا فإن العنوان الرقمي الخارجي المعطى لجهاز داخلي ما يختلف من مرة إلى أخرى .

وأياً كانت طريقة عمل تقنية (NAT) فإن الذي يحدث غالبا أن يقوم إداري شبكة الحاسوب في المنشأة بوضع جهاز يقوم بعملية التحويل (NAT). وكما أسلفنا فإن الجهاز قد يكون جداراً نارياً (Firewall)، أو موجهاً (Router). ولنفترض أنه موجه، ولربط الشبكة الداخلية بشبكة الإنترنت تطلب المنشأة من منظمة (IANA) إعطاءها عنواناً رقمياً مميزاً الذي سميناه سابقاً IP Address)، ويكون هذا العنوان هو عنوان الموجه، وقد تطلب عدة عناوين رقمية مثلما هو الحال في الجهات التي يكون لديها أكثر من خط هاتفي. وفي حال رغبة مستخدم ما داخل الشبكة الداخلية تصفح موقع في شبكة الإنترنت فإن جهاز المستخدم يرسل طلباً إلى الموجه موضحاً فيه العنوان الرقمي للموقع، كما أن الطلب فيه العنوان الرقمي لجهاز المستخدم. وبسبب أن الموقع ليس ضمن الشبكة الداخلية، فإن الموجه يرسل الطلب إلى الموقع، ولكنه قبل ذلك يجري عملية مهمة هي موضوع تقنية (NAT). ولو أن الموجه حاول إرسال الطلب فإن الموقع

الإلكتروني لن يستطيع إرسال الرد ؛ لأن العنوان الرقمي الموجود في الطلب ليس مسجلاً للجهاز الطالب.

وتفادياً لهذه المشكلة يقوم الموجه بتغيير الخانة الخاصة بالعناوين الرقمية للجهاز الطالب في الطلب ، بحيث يصبح محتواها أحد العناوين الرقمية المخصصة من قبل منظمة (IANA) للموجه نفسه ، وبعدها يمكن إرسال الطلب ، وعندما يأتي الرد فإنها توجه إلى العنوان الرقمي للموجه. ونظراً لأن هذا العنوان مسجل لدى (IANA) ، فإن الرد يرسل إلى الموجه ، وهنا يقوم الموجه بمراجعة جدول المتابعة ، ويحدد منه العنوان الرقمي للجهاز الداخلي الذي أرسل ذلك الطلب ، وعندها يغير الموجه خانة العنوان الرقمي في الرد بحيث تحوي العنوان الرقمي للجهاز الطالب ، ثم يُرسل إليه ، وتتكرر العملية كلما حاول مستخدم ما الاتصال بجهاز أو موقع خارج الشبكة الداخلية.

[3] كيف يتحقق الأمن باستخدام (NAT)

قد يتساءل القارئ – بعد كل ما ذكر – عن العلاقة بين أمن المعلومات وتقنية (NAT). والإجابة عن هذا التساؤل تكمن في أن الجهاز الذي يقوم بتطبيق هذه التقنية هو في حقيقة الأمر يقف حائلا بين الشبكة الداخلية وشبكة الإنترنت ، فلا يستطيع من كان مرتبطاً بشبكة الإنترنت معرفة العناوين الرقمية للأجهزة المرتبطة بالشبكة الداخلية ، وهذا يسهم في حمايتها من عدد كبير من أنواع الهجوم التي تُشن باستخدام شبكة الإنترنت بناء على معرفة العناوين الرقمية.

الخلاصة

مع أن فكرة تحويل العناوين الرقمية كان الباعث لها قلة المتح من تلك العناوين فإنها وسيلة لحماية شبكات المعلومات و عزلها عن الاخطار التي تعج بها شبكة

الإنترنـت. و الفكـرة تقـوم علـى إعطـاء عنـاوين رقميـة للأجهـزة الواقعـة علـى الشـبكة الداخلية بحيث لا يمكن استخدامها من الخارج للوصول إلى تلك الأجهزة لوجـود كيـان عازل يقوم بتحويل العناوين الداخلية إلى أخرى خارجية عند رغبـة المستخدمين داخـل الشبكة المحمية الوصول إلى شبكة الإنترنـت. و لـو اعـترض مهـاجم مـا البيانـات القادمـة مـن الأجهـزة الموجـودة علـى الشـبكة الداخليـة فإنـه لا يـرى سـوى العنـاوين الرقميـة الخارجية ، و لكن تلك العناوين توصله فقط إلى ذلـك الكيـان العـازل، وبالتـالي تبقـى الأجهزة الداخلية بعيدا عن متناول المهاجمين.

التحديث التلقائي
Automatic Updates

إن بناء البرمجيات – ومنها أنظمة التشغيل مثل نظام (Windows) – عملية معقدة، ولا تخلو من أخطاء، كما أنها بحاجة إلى تحسينات مستمرة تبعا لتغير ظروف استخدامها وطلبات المستخدمين، وتزايد قدرات الأجهزة؛ ومن ناحية أخرى فإن الحاجة إلى التحسين المستمر يفرضها وجود الثغرات الأمنية التي تكتشف بشكل مستمر في هذه البرمجيات، مما يحتم إغلاق تلك الثغرات قبل أن تُستغل، وإغلاقها يتطلب تحديث البرمجيات. واكتشاف الثغرات قد يكون من قبل الشركة المصنعة للبرنامج، وعندها تقوم الشركة بخطوة استباقية تصدر فيها تحديثا لسد الثغرات الأمنية التي اكتشفتها للتو. وفي أحيان كثيرة يسبق المتطفلون إلى اكتشاف الثغرات، فيطورون برامج سيئة تستغل هذه الثغرات، وتحدث دمارا يتوقف حجمه على عوامل منها: مهارة المتطفل المصمم للبرنامج، وسرعة اكتشاف الثغرات والتعامل معها. وبعبارة أخرى فإن تحسين البرمجيات يفرضها أمران:

(أ) إدخال وظائف جديدة أو تحسين الوظائف الموجودة في البرنامج.

(ب) سد الثغرات الأمنية المكتشفة في البرمجيات للحد من احتمال اختراقها من قبل المتطفلين.

ومطالبة مستخدمي البرمجيات تحديثها بأنفسهم قد يكون صعبا من ناحية عملية، لأن قطاعا عريضا من المستخدمين تنقصه الخبرة الفنية اللازمة لإجراء التحديث، وبدلاً من ذلك وفر عدد من الشركات المصنعة للبرمجيات خاصية التحديث التلقائي أو الآلي (Automatic Updates). ولكي تعمل هذه الخاصية يقوم البرنامج المثبت في الحاسوب بالاتصال بالشركة الأم للت[illegible] وجود أي تحديثات، فإن وُجد منها

شيء بادر البرنامج بتنبيه المستخدم إلى ذلك، وكما هو واضح فإن هذا يتطلب أن يكون الحاسوب موصولا بشبكة الإنترنت. وكما أن تحديث البرمجيات يمكن أن يكون تلقائيا – أي دون أن يبادر المستخدم إلى طلبها – فإن بعض الشركات تعطي المستخدم الخيار في أن يكون التحديث يدوياً، أي بمبادرة من المستخدم الذي عليه أن يذهب إلى الموقع الإلكتروني للشركة المصنعة للبرنامج، ومن ثم يقوم بتحميل (Download) التحديثات التي يختارها.

وعموما تتكون عملية التحديثات التلقائية من المراحل التالية:

(أ) مرحلة اتصال جهاز الحاسوب بالموقع الإلكتروني للشركة المصنعة.

(ب) مرحلة البحث عن التحديثات التي لم يسبق تحميلها إلى جهاز الحاسوب الذي أجرى الاتصال. وهذه الخطوة تتطلب جمع بعض المعلومات عن الحاسوب المتصل؛ وسنعود للحديث عن هذه المسألة لاحقاً.

(جـ) مرحلة تحميل (Download) التحديثات من موقع الشركة إلى جهاز الحاسوب المتصل. ولضمان سلامة المواد التي يجري تحميلها، والتأكد من اكتشاف أي تغيير قد تتعرض له أثناء عملية التحميل، فإن كل مادة تحمل توقيعاً إلكترونياً تضعه الشركة المصنعة. وعلى البرنامج الذي يجري عملية التحديثات تلقائيا التحقق من صحة التوقيع ومطابقته للمادة المنزلة.

(د) مرحلة تنصيب (Installation) التحديثات. لا يبدأ أثر هذه التحديثات إلا بعد أن يجري تنصيبها في الحاسوب.

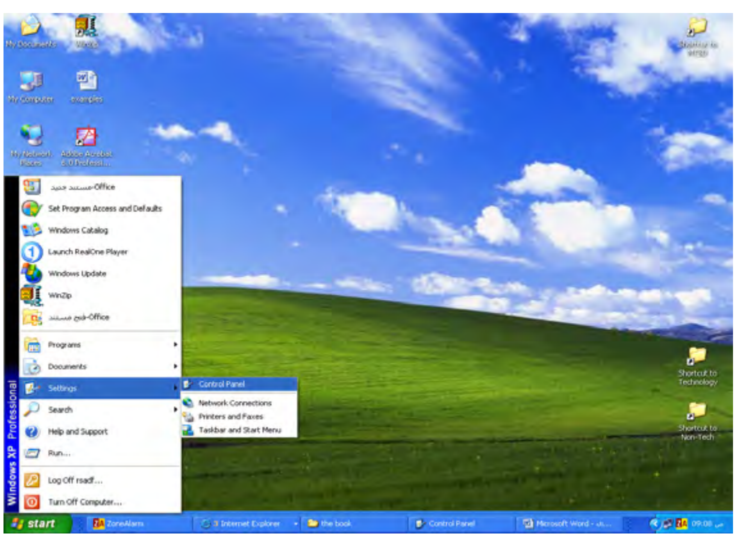
(هـ) مرحلة فصل الاتصال. ولتوضيح كيف تجري التحديثات التلقائية نسوق بعض الأمثلة لبرمجيات تعتمد على هذا الأسلوب، مثل جدران الحماية الشخصية، والبرامج المضادة للفيروسات. غير أن الحديث في هذا الجزء من الكتاب سيكون منصبا

على نظام التشغيل (Windows)، لأنه من أكثر البرمجيات استخداماً، ولأن الأفكار المعروضة تنطبق - إلى حد كبير - على البرمجيات الأخرى.

[1] طريقة عمل التحديثات التلقائية في نظام (Windows)

(أ) كما أسلفنا سيكون وصف طريقة عمل التحديثات التلقائية التي يوفرها نظام التشغيل[1] (Windows). وقبل أن تعمل التحديثات تلقائيا على المستخدم تهيئة النظام لذلك ، و هذا يكون بإجراء الخطوات التالية :

(أ) الذهاب إلى خيار (Control Panel)، وذلك بالنقر على (Start) ، ثم النقر على (Settings)كما في الشكل رقم (21).



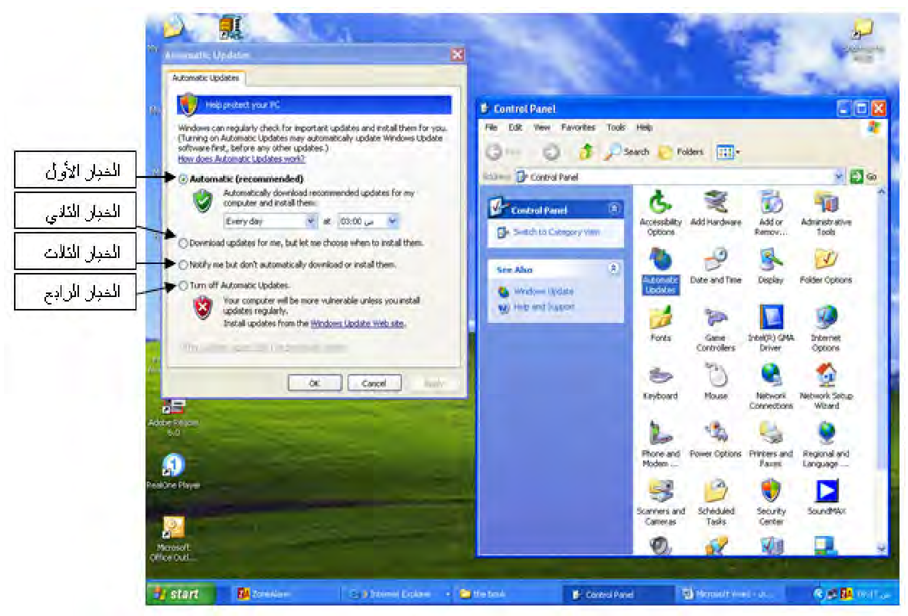
الشكل رقم (21):الوصول إلى خيار التحديثات التلقائية.

(ب) بعد أن تفتح نافذة (Control Panel) يقوم المستخدم بالنقر على أيقونة

---

(1) سنستخدم النسخة (XP Professional) للتمثيل، والنسخ الأخرى من نظام Windows يمكن تهيئتها بطريقة مشابهة.

(Automatic Updates)، كما في الشكل رقم (23–أ)، وهنا يعطي نظام (Windows) المستخدم الخيارات التالية:



الشكل رقم (23–أ): خيارات التحديث التلقائي.

(**1**) **الخيـــار الأول**: أن يقوم النظام بإجراء جميع مراحل عملية التحديثات تلقائيا دون أدنى تدخل من مستخدم الجهاز الذي يمكنه تحديد الوقت المحبذ لإجراء التحديثات، وكذلك تكرار إجرائها. وهذا الخيار هو المحبذ لدى الشركة المصنعة لنظام (Windows).

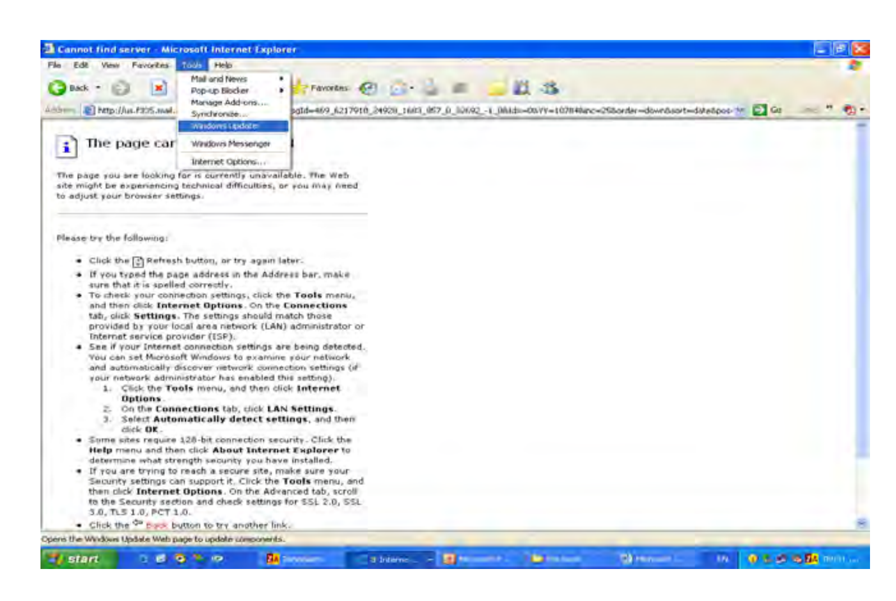
(**2**) **الخيار الثاني**: أن يقوم النظام بإجراء جميع مراحل عملية التحديثات تلقائيا باستثناء تنصيب التحديثات، فيترك تحديد موعد تنصيبها لمستخدم الجهاز.

(**3**) **الخيار الثالث**: أن يقوم النظام بالاتصال بموقع الشركة للبحث عن أي

تحديثات لم يجر تحميلها من قبل، ثم ينبه المستخدم إلى وجود تلك التحديثات، وهنا يكون تحميل هذه التحديثات وتنصيبها رهيناً بموافقة المستخدم.

(**4**) **الخيار الرابع**: إطفاء خاصية التحديثات التلقائية كلياً.

كما أن هناك طريقة أخرى لعمل التحديثات التلقائية، وذلك من خلال المتصفح، وفيها يقوم المستخدم باختيار (Tools)، ثم ينقر على (Windows Updates)، كما هو موضح في الشكل رقم (23–ب)، ومن ثم يتصل بموقع الشركة حيث التحديثات.



الشكل رقم (23–ب): عمل التحديثات التلقائية من خلال المتصفح.

[2] متى تحتاج إلى عمل التحديثات يدويا

إن استخدام طريقة التحديثات التلقائية كفيل بتزويد الحاسوب بآخر إصدارات

الشركة المصنعة من الآتي[1]:

(أ) **التحديثات الأمنية (Security Updates)**: وهذه التحديثات -كما يدل عليها اسمها- هي إصدار لتصحيح ثغرة أمنية معينة اكتشفت في النظام، بحيث إنها إذا لم تُصلح فإنها قد تُستغل للإخلال بأمن النظام، أو المعلومات المخزنة في الحاسوب الذي يعمل عليه النظام.

(ب) **التحديثات الحرجة (Critical Updates)**: وهذه التحديثات هي إصدار لتصحيح خلل في إحدى وظائف النظام المهمة غير المتعلقة بأمن النظام.

(جـ) **الرزم الخدمية (Service Pack)**: هي مجموعة تراكمية من التحديثات، أهم مكوناتها الآتي:

(1) التحديثات الأمنية التي سبق وصفها.

(2) التحديثات الحرجة التي سبق وصفها كذلك.

(3) التعديلات السريعة (Hotfixes) المختصة بأوضاع معينة لاستخدام النظام، وقد تكون خاصة ببعض المستخدمين.

(4) التحديثات الأخرى.

لكن هناك أنواعا أخرى من التحديثات مفيدة للمستخدم، غير أنه للحصول عليها يلزمه أن يقوم بنفسه بزيارة موقع شركة مايكروسوفت. ومن هذه التحديثات:

(أ) إصدارات الترقية (Upgrade) لبعض البرمجيات التي تعمل مع أنظمة مايكروسوفت.

(ب) الأدوات المساعدة (Tools)، وهي برمجيات تساعد في إنجاز مهمة أو مهام مخصصة.

---

(1) موقع: http://support.microsoft.com/?kbid=824684

ومهما كانت طريقة إجراء التحديثات فإن بعضها يتطلب إعادة تشغيل الحاسوب، و في هذه الحالة ينصح المستخدم بتخزين أي عمل لم يسبق تخزينه.

[3] هل إجراء التحديثات التلقائية يمثل خطرا أمنيا في حد ذاته

سبقت الإشارة إلى أن مرحلة البحث عن التحديثات التي لم يسبق تحميلها إلى جهاز الحاسوب الذي أجرى الاتصال تتطلب جمع بعض المعلومات عن الحاسوب المتصل وإرسالها إلى موقع شركة مايكروسوفت، وبحسب شركة مايكروسوفت، فإن هذه المعلومات تشمل الآتي:

(أ) اسم الشركة المصنعة لجهاز الحاسوب، وطراز (Model) الحاسوب.

(ب) رقم نسخة (Version number) لنظام (Windows) المستخدم في الحاسوب المتصل.

(جـ) رقم نسخة برنامج تصفح (Explorer) شبكة الإنترنت المثبت في الحاسوب المتصل.

(د) رقم نسخة أي تحديثات سبق تحميلها إلى الحاسوب المتصل.

(هـ) الرقم المعرف (ID) للأجهزة الداخلة في تكوين الحاسوب.

(و) أوضاع المنطقة، واللغات المحملة (Region and Language Setting).

(ز) رقم التعريف العام (GUID)لنظام (Windows).

(حـ) الرقم المميز للمنتج (Product ID)، والمفتاح الخاص بالمنتج (Product Key).

(ط) اسم الإصدار ورقمه، وتاريخ إصدار النظام الأساس (BIOS).

وتزعم الشركة أن البرنامج الذي يجري التحديثات التلقائية لا يرسل عن المستخدم أيا من المعلومات التالية:

(أ) اسم المستخدم.

(ب) عنوان المستخدم.

(جـ) البريد الإلكتروني للمستخدم.

(د) أي معلومات شخصية تكشف هوية المستخدم.

والشركة تعترف بأنها تسجل العنوان الرقمي المميز (IP Address) للحاسوب الذي استخدم عند الاتصال بموقع الشركة لإجراء التحديث، و لكنها تقول إنها تستخدمه لعمل إحصاءات ذات صبغة عمومية، أي أنها لا تكشف هوية المستخدم. ورغم ما تقوله الشركة فإن للمستخدم كل الحق إذا ساوره القلق حول تأثير استخدام التحديثات التلقائية، بل التحديثات عموما على أمن المعلومات التي يعمل على حمايتها. وقد ظهرت أبحاث و مقالات تعزز هذا القلق[1].

الخلاصـــة

تأتي أهمية التحديثات التلقائية من أن البرامج لا يمكن أن تخلو من الأخطاء، و شواهد الواقع تدل بما لا يدع مجالا للشك على أن كثيراً من حوادث اختراق المنظومات المعلوماتية إنما كان ممكنا لوجود تلك الأخطاء، و تسعى الشركات المصنعة للبرامج إلى إصدار تحديثات لمعالجة تلك الأخطاء. و لتوفير الحماية لأنظمة المعلومات يجب تنزيل تلك التحديثات لإبقاء البرامج في أفضل أوضاعها، وبالتالي تفويت الفرصة على المتربصين. و قد استعرضنا كيف يمكن إجراء تلك التحديثات بطريقة آلية في أحد أكثر البرامج شيوعا، وهو نظام التشغيل (Windows) من شركة مايكروسوفت.

---

(1) انظر على سبيل المثال مقال: M$ Windows XP Professional Bugging Device؟ في الموقع:
http://www.indymedia.org.uk/en/2004/10/298702.html

التشـــــفـــــير
Encryption

هل كل ملفاتك تحمـل نفـس مسـتوى السـرية و الخصوصـية ؛ هـل أنـت الوحيـد الذي يتعامل مع حاسوبك ؛ وهل هو في مكان آمن يضمن عدم سرقة الملفات الموجودة فيه؟ إذا كان الجواب بنعم فأنت لا تحتاج إلى تشـفير للملفـات. أمـا إذا كنـت غـير ذلـك فيلزمك تشفيرها لحمايتها من تطفل الغير. والتشفير عملية قديمة يقصد بها تحوير محتـوى الرسالة (أو أي محتوى) بشـكل يصـعب علـى الغـير معرفـة المحتـوى الأسـاس. ومجـازاً لا يسـتطيع أحـد معرفـة المحتـوى، أو إعادتـه إلى وضـعه الأصـلي إلا مـن يعـرف كيـف تم تحـويره. فتحـوير المحتـوى أو تشـفيره يـتم بوجـود متطلـبين: الأول هـو طريقـة التحـوير (الخوارزمية)، والآخر هو المفتاح السري الذي اسـتخدم للتشـفير وفـك التشـفير، وهـو سري على اسمه يفترض ألا يعرفه إلا من شفر البيانات.

التشفير سلاح ذو حدين، يوفر لك حماية لمحتوى البيانـات، لكـن إذا فُقـد المفتاح السري، أو البرنامج الذي شفر المحتوى فلا فائدة ترجـى مـن وراء المحتـوى المشفر. لذا يلزم المحافظة على المفتاح السري في مكان غير مكان المحتوى المشـفر ، وفي حال استخدام كلمة مرور للتشفير، احرص على اختيار كلمة مرور قوية.

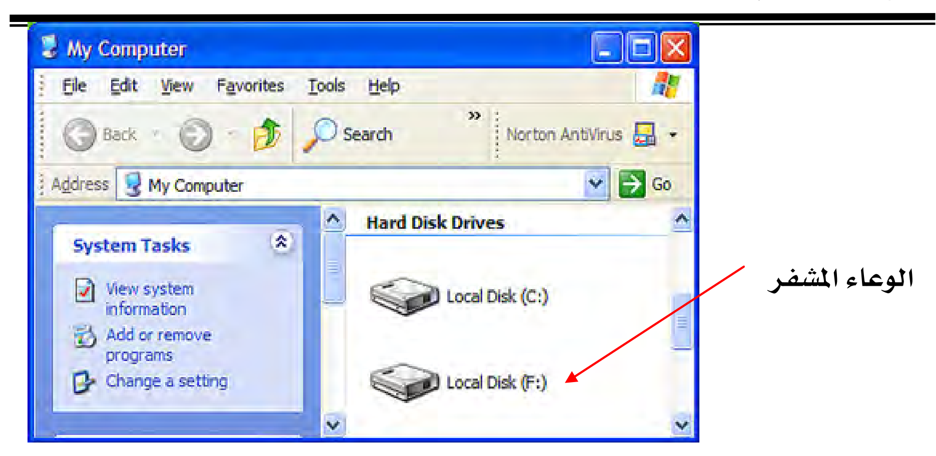
[1] بعض أنواع برامج التشفير

هناك العديد من برامج التشفير ، منها المجانية ، ومنها التجاري، منها الشخصي ومنهـا علـى مسـتوى الشـركات والمنظمـات. ويختلـف عمـل كـل واحـد منهـا. فـبعض البرامج تشفر ملفاً ملفاً، وبعض البرامج تتيح لك تشفير مجلدٍ كاملٍ بما فيه مرة واحـدة، وبعض البرامج توفر لك وعاء يمكنك م [illegible] الفات المراد تشفيرها فيه، وهي تقـوم بالتشفير التلقائي. وفي الجزء التالي سوف [illegible] ين من أنواع برامج التشفير، وطريقة

عملهما، كذلك سنتحدث عن خاصية التشفير المتضمنة مع أنظمة التشغيل ويندوز، وكيفية عملها.

أ-برنامج Best Crypt

يعد هذا البرنامج من البرامج المشهورة في التشفير، ويعمل بطريقة متميزة. كما يقوم هذا البرنامج باحتجاز مساحة محددة من القرص الصلب، ويكوّن ما يعرف بالوعاء المشفر (Container)، أو محرك الأقراص الافتراضي (Virtual Drive)، وهذا الوعاء يحاكي المشفر، أي محرك أقراص صلب، وله مسمى مثل محرك الأقراص الصلب، انظر الشكل (24). والفائدة من الوعاء المشفر هو سهولة التشفير، فبمجرد فتح الوعاء يمكنك نقل ملفات إليه (ويعد هنا تشفيراً)، أو نقل ملفات منه (ويعد هنا فك التشفير). لاحظ كيف تمت عملية التشفير، مجرد نقل ملفات فقط دون أوامر، ولا إدخال كلمات مرور أو غيرها. بالإضافة إلى سهولة التشفير، يمكن للبرامج الموجودة في الحاسوب (مثل برنامج محرر النصوص، والجداول) التعامل مع الملفات المشفرة، وكأنها لم تشفر، وهذه فائدة عظيمة، كون بعض برامج التشفير الأخرى تلزمك من فك التشفير أولاً، ثم التعامل معها. وعند الرغبة في إخفاء هذا الوعاء فما عليك سوى تعطيل الوعاء وغلقه بنقرتين على الفأرة، وكذلك عند فتح الوعاء مرة أخرى يمكن نقل الوعاء على قرص متحرك مثل القرص الضوئي (CD-ROM)، وفك تشفيره في جهاز آخر؛ ولكن لابد هنا من أمرين: أولهما: وجود برنامج Best Crypt على الحاسوب المراد فتح الوعاء فيه، والآخر: هو معرفة كلمة المرور لفتح الوعاء. في الجزء التالي سنقوم بشرح طريقة عمل البرنامج.



الشكل (**24**): شكل الوعاء المشفر.

يمكنك الحصول على نسخة من البرنامج صالحة لمدة 30 يوماً مجاناً من موقع الشركة المطورة على الرابط التالي : http://www.jetico.com/

تكوين وعاء التشفير(Container): بعد تنصيب البرنامج ، عليك تكوين وعاء تشفير باتباع الخطوات التالية :

1- انقر بزر الفأرة الأيمن على أيقونة البرنامج ، كما هو موضح في الشكل (25).

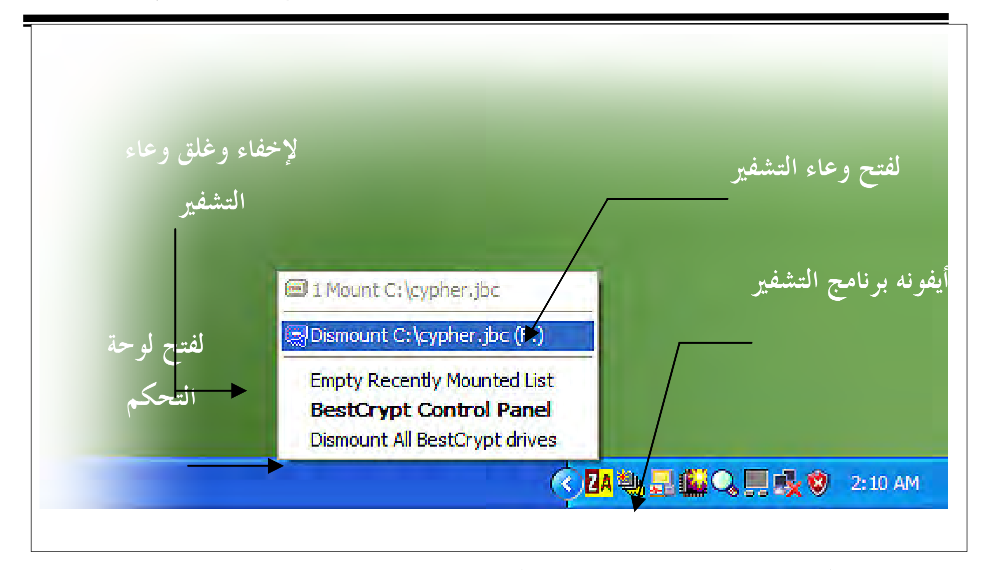
2- بعد ظهور القائمة اختر الخيار "BestCrypt Control Panel" لفتح لوحة التحكم.

3- ستظهر لوحة التحكم كما في الشكل 26.

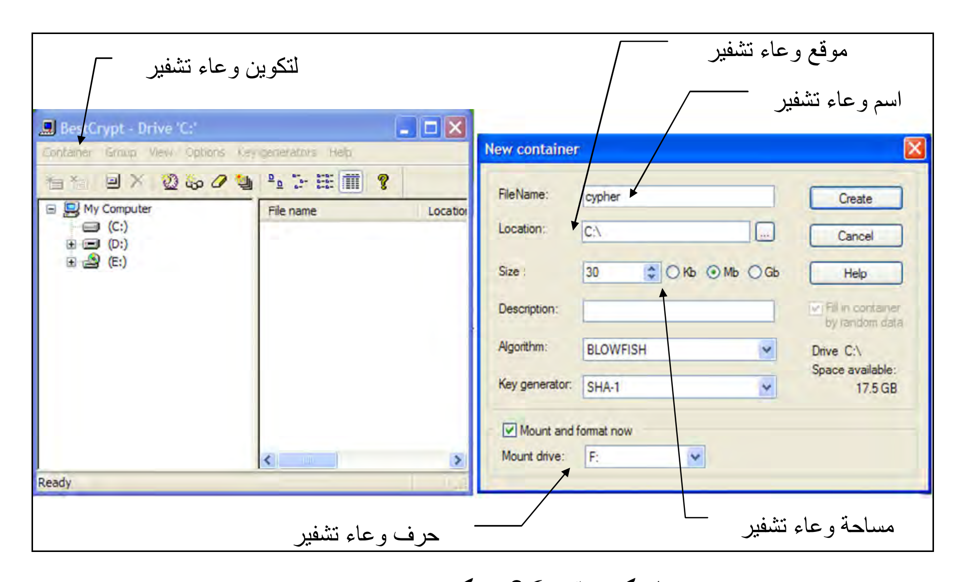
4- اختر Container ثم New Container.

5- اكتب اسماً للوعاء ، وموقع تخزينه ، وحجمه ، ثم اختر حرفا للدلالة عليه من بين محركات الأقراص الأخرى.

6- انقر على زر Create.

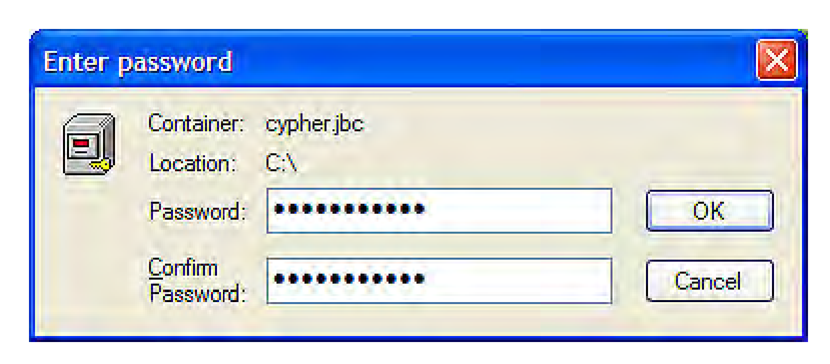


الشكل رقم (25): القائمة الفرعية لأوامر برنامج **Best Crypt**.



الشكل رقم (26): تكوين وعاء تشفير.

7- سيظهر مربع حوار(كما في الشكل27) لطلب كلمة مرور خاصة بالوعاء، وهذه سوف تحتاجها عند فتح الوعاء.



الشكل رقم (27): كلمة مرور للوعاء المشفر.

8- بعد ذلك سيطلب البرنامج منك تكوين ما يسمى بذرة التشفير (Seed)، وذلك بالنقر على لوحة المفاتيح بشكل عشوائي حتى يكتمل الخط الأخضر، ولا يلزمك حفظ حروف البذرة.

9- بعد ذلك سيظهر لك مربع حوار لتهيئة (Format) الوعاء على أنه قرص تخزين جديد، اضغط على زر (Start) ، أو ابدأ لتهيئة الوعاء.

10- عند الانتهاء، اضغط على زر إغلاق (Close).

11- الآن تكوّن في جهازك وعاء تشفير.

(1) فتح وعاء التشفير أو تفعيله

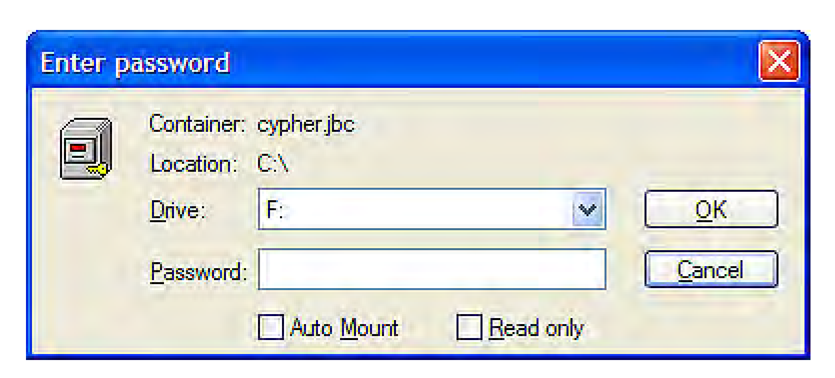
يلزمك لاستخدام وعاء التشفير بعد تكوينه وعند تشغيل الجهاز مخفياً فتحه، وذلك بإتباع الخطوات التالية:

1- انقر بالزر الأيمن في الفأرة على أيقونة برنامج التشفير.

2- ستظهر لك قائمة كما في الشكل (25)، اختر: <اسم الوعاء> Mount.

3- بالطبع، ولسرية المعلومات التي في الوعاء، سيطلب منك التأكد من هويتك، وذلك بطلب كلمة المرور الخاصة بالوعاء المراد فتحة، كما في الشكل (28).

4- يمكنك أيضاً اختيار حرف الوعاء.



الشكل رقم (**28**): كلمة مرور لوعاء التشفير .

(2) لإخفاء الوعاء

يمكنك إخفاء الوعاء عند عدم الاستخدام، أو عند غلق الجهاز، وذلك باتباع الخطوات التالية:

1- انقر بالزر الأيمن في الفأرة على أيقونة برنامج التشفير.

2- ستظهر لك قائمة كما في الشكل(25)، اختر: <اسم الوعاء> Dismount.

لمزيد من المعلومات عن البرنامج، يمكنك مراجعة دليل المستخدم الذي في البرنامج، أو زيارة موقع الشركة.

ب- برنامج Fine Crypt

يحتوي هذا البرنامج على عديد من المميزات، مما قد يثري عمل البرنامج، وفي

الوقت نفسه يعقد عمله. لذا سوف نشرح الحد الأدنى من عمل البرنامج للتشفير، ونترك باقي المميزات لمن يريد الاستزادة، وذلك بالرجوع لدليل البرنامج.

يعتمد التشفير في هذا البرنامج على أي من كلمة مرور أو مفتاح تشفير يمكن تكوينه من خلال البرنامج، وهو أقوى من كلمة المرور. هذا البرنامج يعمل بطريقة مختلفة عن Best Crypt، والذي يوفر وعاء للتشفير، ولا يطلب كلمة المرور إلا مرة واحدة عند فتح الوعاء. أما Fine Crypt فإنه يستلزم كلمة المرور، أو مفتاح التشفير كلما أردت التشفير، أو فك التشفير، إلا إذا استخدمت ما يسمى كلمة مرور الجلسة (Session Pass)، أو مفتاح تشفير الجلسة (Session encryption key)، وهو اعتماد البرنامج للتشفير، وفك التشفير على كلمة مرور، أو مفتاح تشفير مخزن في ذاكرة الجهاز لمدة معينة بدلاً من سؤالك كل مرة. ويتميز هذا البرنامج عن Best Crypt بأنه يتيح وفك تشفير الملف المشفر وإرساله لأي شخص، حتى وإن لم يملك نسخة من البرنامج. يمكن الحصول على نسخة محدودة المميزات مجانا من موقع الشركة على الرابط:

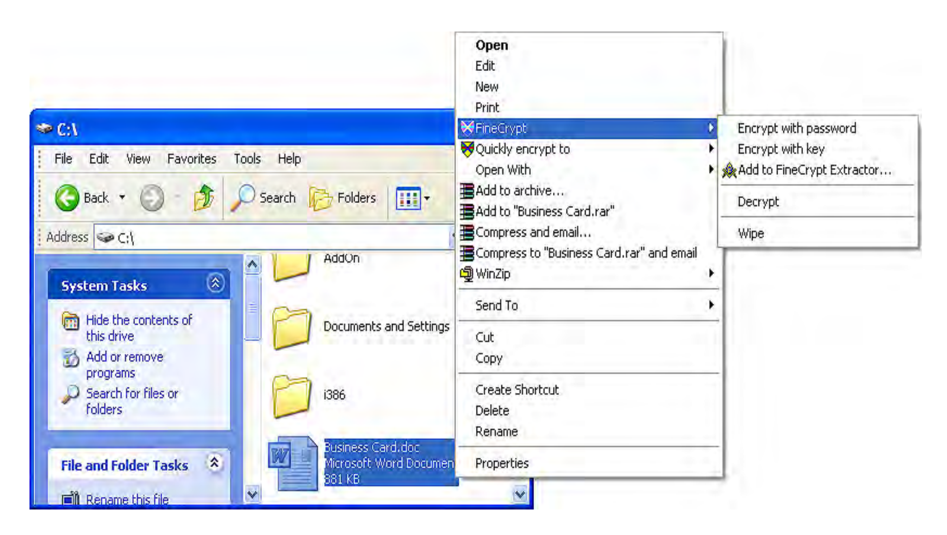
http://www.finecrypt.net/

(أ) تشفير ملف أو مجلد

يمكنك تشفير ملف، أو عدة ملفات، أو حتى مجلد بكامله بعدة طرق؛ لكن سنقتصر في الشرح فقط على طريقة واحدة كما يلي:

(1) بعد تنصيب البرنامج اختر الملف أو المجلد الذي تريد تشفيره من خلال مستكشف الويندوز، وانقر على الزر الأيمن للفأرة.

(2) تظهر لك قائمة كما في الشكل (29).



الشكل رقم (29): القائمة الفرعية لبرنامج FineCrypt .

(3) اختر Fine Crypt ، ثـم نظهـر لك ثلاثة خيـارات هي : إمـا التشفير بكلمة مرور ، أو بمفتاح تشفير ، أو التشفير المستقل عن البرنامج لنقله وحده لحاسوبٍ آخر. وسنتطرق لكل طريق على حدة.

*** للتشفير باستخدام كلمة المرور اختر "Encrypt with password"**

1- أدخل كلمة مرور ثم اختر موافق.

2- اضغط على زر "Encrypt" كما في الشكل (30).

3- بعد ذلك سيظهر لك الملف مشفراً على شكل قفل ذهبي في مجلد الملف الأصلي نفسه.

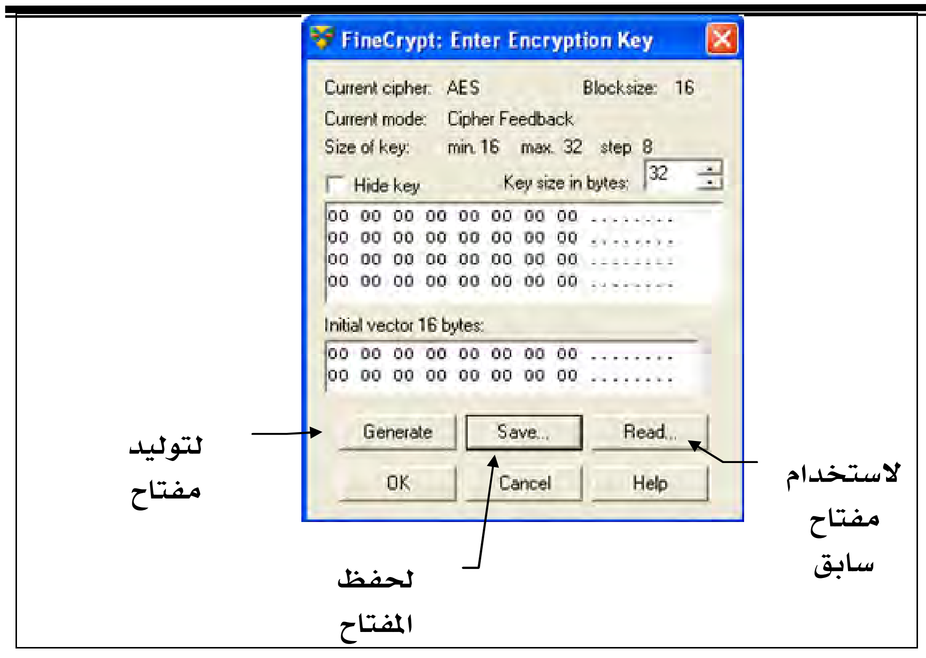


الشكل رقم (**30**): واجهة برنامج **Fine Crypt** .

*** أما إذا اخترت التشفير بمفتاح تشفير فعليك اختيار "Encrypt with Key"**

1- سيظهر لك مربع حوار لتحديد مفتاح التشفير، وأنت أمام خيارين : إما أن تولد مفتاحاً جديداً ثم تحفظه ، أو أن تستخدم مفتاحاً سابقاً كما هو مبين في الشكل (31).

2- انقر على زر موافق (OK)، ثم اتبع خطوة رقم (6).



الشكل رقم (**31**): كتابة مفتاح التشفير.

*** إذا أردت تشفير ملف مستقل عن البرنامج فاختر**

"Add to Fine Crypt Extractor…"

1- اكتب كلمة مرور لتشفير الملف، ثم اتبع خطوة رقم 6.

2- سيظهر لك ملف مشفر على هيئة تنفيذية (Exe) في المجلد نفسه.

3- يمكنك نقله لأي حاسوب، حتى ولو لم يكن لديه البرنامج نفسه، ولكن لابد من معرفة كلمة المرور.

(ب) فك التشفير

يمكن فك التشفير بإتباع الخطوات التالية:

1- اختر الملف أو المجلد الذي تريد فك تشفيره من خلال مستكشف الويندوز، ثم انقر على الزر الأيمن للفأرة.

2- ستظهر لك قائمة كما في الشكل(29).

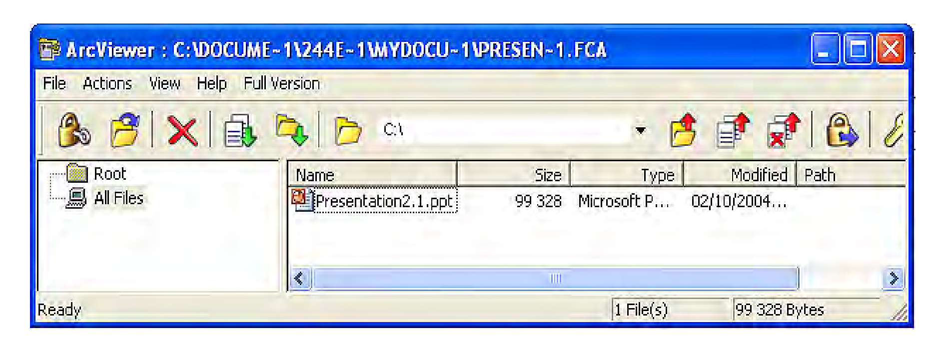
3- اختر Fine Crypt ثم Decrypt.

4- إذا كان تشفير الملف بكلمة مرور فأدخلها ؛ أما إذا كان تشفيره بمفتاح فعليك تحديد مفتاح التشفير بالنقر على زر Read.

5- سيظهر لك مربع حوار لتحديد المفتاح ، حدد المفتاح ثم انقر على زر موافق.

6- انقر على زر OK.

7- نظهر لك شاشة لمحتوى الملف أو المجلد المشفر كما في الشكل (32).



الشكل رقم (32): شاشة لمحتوى الملف أو المجلد المشفر.

8- حدد الملف المراد فك تشفيره ، ثم من القائمة اختر Action ، ثم Decrypt Selected Files ، أو انقر على زر F5.

9- عند ذلك تم فك تشفير الملف ، أو المجلد في المجلد نفسه الذي فيه الملف ، أو المجلد المشفر.

هناك عديد من المميزات والخدمات التي يقدمها البرنامجان ، لكننا اقتصرنا في هذا الكتاب على الخدمات والخطوات الأساسية من تشفير وفك تشفير ، وتركنا باقي الخصائص للمستخدم للتعرف عليها ، من خلال دليل المستخدم المرفق مع البرنامجين.

[2] تشفير الويندوز

توفر أنظمة التشغيل ويندوز 2000، ويندوز إكس بي للمحترفين فقط، وويندوز 2003 إمكانية تشفير الملفات والمجلدات بطريقة سهلة للغاية. لكن لابد من استخدام نظام NTFS لوحدة التخزين، حتى يتسنى لك التشفير.

تشفير الملفات/المجلدات يتم باتباع الخطوات التالية:

1- حدد الملف/المجلد المراد تشفيره، ثم انقر على الزر الأيمن للفأرة.

2- انقر على **خصائص**.

3- سيظهر لك مربع حوار كما في الشكل (33).

4- في صفحة عام انقر على زر **خيارات متقدمة**.

5- علّم على خيار **تشفير المحتويات لتأمين البيانات**.

يمكنك التشفير بطريقة أسهل من ذلك بأن تفعل الخطوات التالية نفسها لتشفير مجلد محدد، ثم تقوم بإدراج أي ملف أو مجلد تريد تشفيره داخل المجلد المشفر، وسيكون كل ما بداخل هذا المجلد المشفر مشفراً.

فك التشفير عملية عكسية للتشفير، وذلك بعدم تحديد خيار **تشفير المحتويات لتأمين البيانات**. ويمكن للبرامج من فتح الملف وكأنه لم يشفر. لكن لأن الملف يمكن فتحه إذا كان المستخدم للنظام هو من قام بتشفيره، أو أنه مخول لذلك، فينبغي عدم تشفير محرك وحدة التخزين التي تحتوي على ملفات النظام، التي قد يحتاجها مستخدمون آخرون، وقد تقلل من سرعة استجابة الحاسوب. أيضا يمكن ضغط الملف أو تشفيره، ولا يمكن الجمع بينهما، وكذلك نقل الملف المشفر إلى وحدة تخزين لا تستخدم NTFS مثل القرص المرن فإن التشفير سوف يلغى.



الشكل رقم (**33**): **طريقة تشفير ملف في نظام ويندوز.**

يمكنك تحديد الأشخاص المخولين لفك تشفير الملف، أو المجلد المشفر، أو فتح أحدهما باتباع الخطوات التالية:

1- بعد تشفير الملف قم باتباع الخطوات السابقة من 1- 4، ثم انقر على زر **التفاصيل**.

2- سيظهر لك مربع حوار مثل شكل (34).

3- يتكون مربع الحوار من قائمتين، الأولى تحتوي على الأشخاص الذين يمكنهم فك تشفير الملف أو المجلد.

4- لإضافة مستخدم، انقر على زر **إضافة**.

5- حدد المستخدمين، ثم انقر على زر **موافق**.

تفاصيل التشفير لـ C:\Presentation2.1.ppt

المستخدمون الذين يمكنهم الوصول إلى هذا الملف في سرية:

اسم المستخدم	بصمة إبهام الشهادة
خالد(خالد@SOLIMAN)	DDFC 360A C6AC D0 ١٠٨٥...

إضافة ... | إزالة

عوامل استرداد البيانات لهذا الملف كما تم تعريفها بواسطة نهج الاسترداد:

اسم عميل الاسترداد	بصمة إبهام الشه...
Administrator	٥1AD 7F3C B2D...

موافق | إلغاء الأمر

الشكل رقم (**34**): **تفاصيل تشفير ملف.**

الخلاصة

التشفير وسيلة لحماية سرية المعلومات، فلا يطلع عليها من ليس مخولا بذلك. و يوجد عدد كبير من البرامج و المعدات التي تقدم خدمة التشفير، و هي في متناول المستخدم، واستخدامها لا يتطلب معرفة عميقة بتقنيات المعلومات، كما إنها توفر قدرا معقولا من الحماية ضد المهاجمين العاديين.

طمس البيانات
Wiping

يظن المبتدئون في تعلم الحاسوب أنه بمجرد حذف ملف ما فإنه يكون قد فُقِدَ نهائياً، ولا يعلمون أن الملف قد تم نقله (منطقياً) إلى سلة المحذوفات، ويمكن استرجاعه. ويظن كثير من المستخدمين أن حذف الملف من سلة المحذوفات هو الإتلاف النهائي لذاك الملف، و هذا غير صحيح. فحذف ملف ما من وحدة التخزين يتم بحذف المؤشر الذي يدل عليه وليس الملف نفسه، أي أن محتويات الملف تظل في وحدة التخزين، ولكن على هيئة مساحة فارغة يمكن الكتابة عليها. ولما كان كذلك فإنه يمكن بواسطة برامج استرجاع متخصصة استرجاع ذلك الملف. لقد تمكنت مجموعة من الأشخاص بعد شراء عدد من وحدات التخزين المستعملة من الحراج والتي تعود ملكيتها إلى أشخاص، أو شركات، أو جهات حكومية من استرجاع محتويات تلك الوحدات، والحصول على معلومات ذات قيمة، وبعضها سري، لأنه لم يتم طمس البيانات في تلك الوحدات بالشكل المطلوب. وعملية طمس البيانات في وحدات التخزين تتم بالكتابة المتكررة على البيانات الموجودة ببيانات عشوائية وبعدة مرات. وهناك معايير معروفة لطمس البيانات. فمثلاً معيار وزارة الدفاع الأمريكية يتطلب طمس البيانات بالكتابة عليها 7 مرات، ومعيار بيتر قتمن (Peter Gutmann) يتطلب الكتابة 35 مرة.

هناك ثلاثة أنواع لطمس البيانات، أولها هو طمس الملف عند حذفه، وثانيها هو طمس المساحة الفارغة في وحدة التخزين، وثالثها طمس ما يعرف بملف المبادلة (Swap File)، وهو ملف خاص بنظام التشغيل، يستخدم لدعم الذاكرة الافتراضية. فعند فتح ملف قد يتم نسخه إلى ملف المبادلة والذي يمكن

قراءة محتواه. والخطير في الأمر أنه حتى لو استخدمت ملف مشفراً ثم فتحته فإنه قد يُحتفظ بالملف المفتوح غير المشفر لمدة ما في ملف المقايضة.

عند التعامل مع ملفات سرية، أو عند التخلص من وحدة التخزين فإنه يستوجب عليك التأكد من طمس جميع البيانات المحذوفة. وهناك عدة برامج الطمس، لكن سوف نقتصر على عمليات الطمس المقدمة مع برنامجي التشفير اللذين ذكرناهما آنفا.

[1] Best Crypt

عند حذف ملف مهم و أردت طمسه نهائياً قم بالآتي:

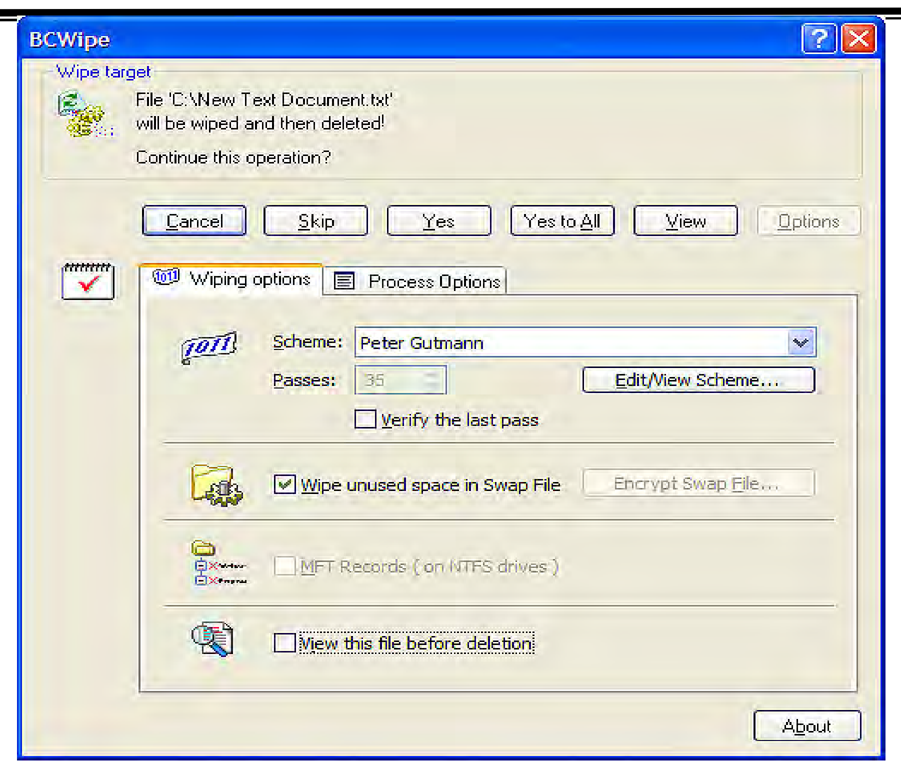
(1) قم بتنصيب برنامج Best Crypt أو BCWipe.

(2) حدد الملف المراد طمسه من مستكشف الويندوز، ثم انقر على الزر الأيمن للفأرة.

(3) اختر Delete with wiping.

(4) سيظهر لك مربع حوار، انقر على Option لإظهار خيارات الطمس، كما في الشكل (35).

(5) يمكنك من الخيارات أن تحدد معيار الطمس، وهل تريد حذف المساحة غير المستغلة من ملف المقايضة.



الشكل رقم (**35**): خيارات الطمس.

لطمس المساحة المتاحة على وحدة التخزين قم بالآتي :

(1) حدد وحدة التخزين (مثل C:\).

(2) انقر على الزر الأيمن للفأرة.

(3) اختر .Wipe free spaces with BCWipe

(4) سيظهر لك مربع حوار لاختيار معيار الطمس وبعض الخيارات.

(5) بعد تحديد الخيارات المطلوبة انقر على زر OK.

(6) لاحظ عدد الساعات التقريبية لإنهاء العملية في أسفل مربع الحوار.

[2] Fine Crypt

يمكنك الاستفادة من خدمة طمس المعلومات من خلال استخدام برنـامج Fine Crypt باتباع الخطوات التالية :

(1) حدد الملف أو المجلد الذي تود طمسه ، وانقر بالزر الأيمن للفأرة.

(2) ستظهر لك قائمة، اختر Fine Crypt ، ثم Wipe.

(3) اختر OK.

يمكنك تحديد عدد دورات الطمس باتباع الخطوات التالية :

1- انقر على **ابدأ**.

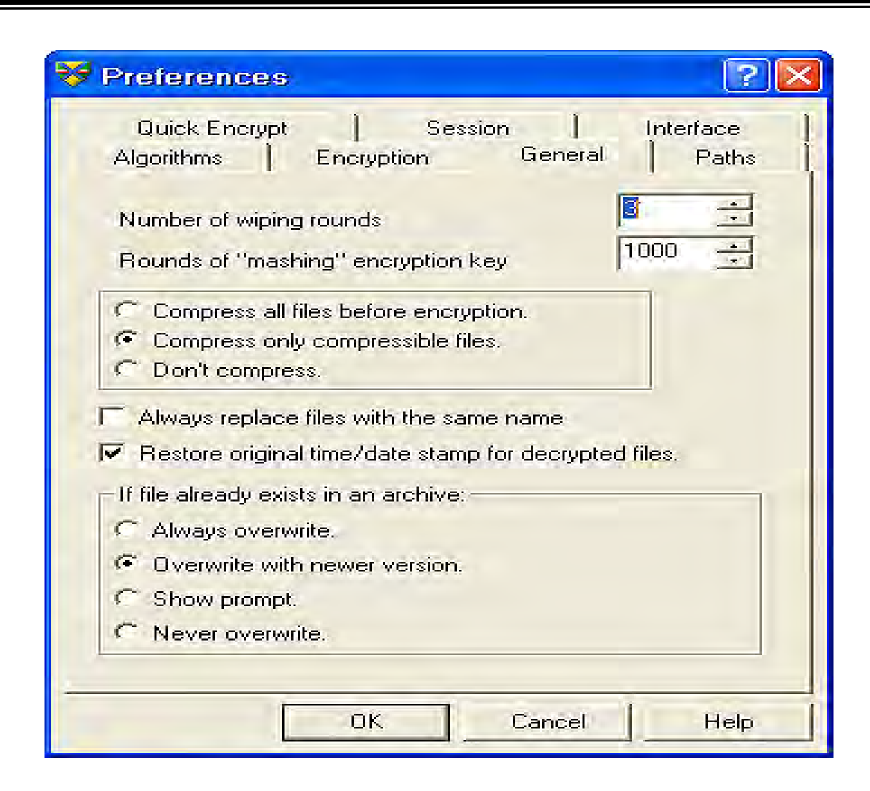
2- انقر على **كافة البرامج**.

3- انقر على FineCrypt.

4- انقر على Encryption Preferences.

5- سيظهر لك مربع حوار ، اضغط على صفحة General كما في الشكل (36).

6- يمكنك تحديد عدد الدورات في أعلى الصفحة.



الشكل رقم (36): خيارات المسح.

الخلاصة

تذكر دائما أن حذف المعلومات لا يعني أنها أصبحت بعيدة المنال من وجهة نظر المهاجم. و لكي نجعلها بعيدة المنال بحق فلا بد من استخدام التقنيات التي تطمسها إلى غير رجعة.

المشاركة في الملفات و المجلدات
Files and Folders Sharing

في بيئة يتعدد فيها المستخدمون يتحتم اشتراك بعض الملفات أو المجلدات بين مستخدمين معينين، لكن في الوقت نفسه لابد من التحكم في نوعية مشاركة كل مستخدم لكل ملف أو مجلد لضمان سرية الملفات.

هناك نوعان من الصلاحيات للتحكم في المشاركة:

الأول: المشاركة من خلال الشبكة.

والآخر: المشاركة المباشرة على النظام نفسه، وسوف نتطرق لكليهما بشكل مبسط ومختصر، نظراً لتعقيد الثاني .

[1] المشاركة في الملفات والمجلدات من خلال الشبكة

في حالة اتصالك بشبكة معلوماتية، سواء في العمل أو البيت، فإنه يمكنك إتاحة المشاركة للملفات والمجلدات للمستخدمين من خلال الشبكة، ويمكنك فعل ذلك باتباع الخطوات التالية:

(1) حدد المجلد (وليس الملف) المراد إشراك غيرك في الوصول إليه.

(2) انقر على الزر الأيمن للفأرة، ثم اختر خصائص.

(3) سيظهر مربع حوار مثل الشكل (37).

(4) اختر صفحة مشاركة.

(5) اختر مشاركة هذا المجلد.

(6) انقر على زر أذونات.



الشكل رقم (**37**): خيارات المشاركة.

(7) سيظهر لك مربع حوار مثل الشكل (38).

(8) هناك مربعان: الأول: للمستخدمين المخولين، والآخر: نوعية الصلاحية المعطاة لكل مستخدم. وبشكل افتراضي مبدئي، تعطى مجموعة Everyone (كل المستخدمين) صلاحية قراءة، وفي بعض الأنظمة تعطى صلاحية تحكم كامل، لذا يجب الانتباه لذلك، وحذف تلك المجموعة.

(9) بعد حذف مجموعة Everyone فليست لأحد قدرة على مشاركتك هذا

المجلد. لذا يجب تحديد الأشخاص، أو المجموعات المخولة لمشاركة المجلد، ويمكنك فعل ذلك بالنقر على زر **إضافة**، ثم تحديد الأشخاص، أو المجموعات.

(10) بعد اختيار الأشخاص، أو المجموعات، يتوجب عليك تحديد نوع الصلاحية الممنوحة. حدد الشخص، أو المجموعة، ثم اختر من الصلاحيات التي في المربع الثاني، وهي كالتالي:

(أ) تحكم كامل: تحكم كامل (كتابة وقراءة وحذف وتنفيذ وغيرها) لجميع المجلدات والملفات داخل هذا المجلد.

(ب) تغيير: قراءة وكتابة فقط لجميع المجلدات والملفات داخل هذا المجلد.

(جـ) قراءة: قراءة فقط لجميع المجلدات والملفات داخل هذا المجلد.



الشكل (38): خيارات الصلاحيات.

[2] المشاركة في الملفات و المجلدات المباشرة على نفس النظام

قد يستخدم الجهاز أكثر من مستخدم. لذا نحتاج إلى طريقة للتحكم في الصلاحيات الممنوحة لكل مستخدم. سواء بإعطاء صلاحية معينة، أو حجب صلاحية أخرى. وهذه الصلاحيات تنطبق على الوصول المباشر للمستخدمين الموجودين في الحاسوب الواحد، أو المستخدمين الواصلين من خلال الشبكة. وللتحكم في الصلاحيات الممنوحة يمكنك إتباع الخطوات التالية:

1- حدد الملف أو المجلد المراد تحديد الصلاحية.

2- انقر على الزر الأيمن للفأرة، ثم اختر **خصائص**.

3- سيظهر لك مربع حوار، كما في الشكل (39).

4- اختر صفحة **أمان**.

5- هناك مربعان: الأول: للمستخدمين المخولين، والآخر: نوعية الصلاحية المعطاة لكل مستخدم. حدد المستخدم، ثم قم بتغيير الصلاحية الممنوحة، وذلك بالسماح أو الرفض.

[3] نصائح

أعط أقل صلاحية ممكنة للمستخدمين. مثلاً إذا كان المستخدم يتطلب قراءة الملفات، فلا تعطه صلاحيات القراءة والكتابة.

أعط الصلاحية للمجموعة، وليس للأشخاص. وهذه النصيحة مهمة في حالة كان عدد المستخدمين كثيراً .

الصلاحيات تُتوارث من الأعلى إلى الأسفل، أي أن الصلاحية الخاصة بالمجلد تعمل على جميع الملفات والمجلدات داخل ذلك المجلد، لذا احرص على إعطاء الصلاحيات للمستويات العليا لتسهيل إدارة الصلاحيات.



الشكل رقم (39): خيارات الأمان.

الخلاصة

المشاركة في الملفات إحدى وسائل تسهيل العمل، و زيادة الإنتاج، ولكنها في الوقت ذاته تفتح ثغرات أمنية في منظومة المعلومات، ولذلك لابد أن يتعرف المسخدم على الطريقة الصحيحة للاستفادة من هذه الوسيلة، وتوقي أخطارها في آن واحد.

التخزين الاحتياطي
Backup

تخيل أن جميع ملفاتك التي جمعتها خلال سنين قد محيت من حاسوبك فجأة لسبب أو لآخر. ماذا تقول عندها؟... يا ليتني حفظت نسخة من ملفاتي خارج الحاسوب، وهو ما يسمى التخزين الاحتياطي. سنترك ذكر أهمية التخزين الاحتياطي لبديهيتها، وسنتكلم عن مكونات التخزين الاحتياطي، وكيفية استخدام برنامج للتخزين.

يتألف التخزين الاحتياطي من:

1- البيانات المراد تخزينها من ملفات ومجلدات.

2- وسيلة التخزين مثل الأقراص المرنة، والمدمجة، والصلبة، والمخصصة للتخزين. وتختلف الوسائط بحسب سعتها، وسعرها، وعمرها الافتراضي.

3- برنامج التخزين الذي يقوم بتخزين واسترجاعها البيانات.

[1] برنامج التخزين الاحتياطي

هناك عديد من برامج التخزين، ولعل من أفضلها برنامج Norton Ghost، والذي يأخذ نسخة (صورة مماثلة) كاملة لما في الجهاز من برامج وملفات. لكن سنقتصر في هذا الجزء على برنامج النسخ الاحتياطي المدمج مع نظام التشغيل ويندوز.

[2] عمل نسخة احتياطية

1- انقر على **ابدأ | كافة البرامج | البرامج الملحقة | أدوات النظام | النسخ الاحتياطي**.

2- سيظهر لك معالج النسخ الاحتياطي، أو الاستعادة. انقر على **التالي**.

3- حدد **نسخ الملفات والإعدادات احتياطياً**، ثم انقر على **التالي**.

4- اختر نوع التخزين (النسخ ... مجلدات محددة اختر **اختيار ما سيتم**

نسخه احتياطياً).

5- حدد مكان حفظ النسخة واسمها.

6- أنه المعالج ليبدأ بالنسخ.

7- في حالة اختيار نوع التخزين **اختيار ما سيتم نسخه احتياطياً**، فإنه يمكنك تحديد نوع التخزين من بين عادي، نسخ، تزايدي، تفاضلي، يومي؛ وذلك بالنقر على زر **خيارات متقدمة** في الصفحة النهائية للمعالج.

[3] استرجاع نسخة احتياطية

1- انقر على: **ابدأ | كافة البرامج | البرامج الملحقة | أدوات النظام | النسخ الاحتياطي**.

2- سيظهر لك معالج النسخ الاحتياطي، أو الاستعادة. انقر على **التالي**.

3- حدد **استعادة الملفات والإعدادات**، ثم انقر على **التالي**.

4- حدد النسخة الاحتياطية بالنقر على زر **استعراض**، ويمكنك تحديد ملف/ مجلد أو عدة ملفات/ مجلدات.

5- انقر على **التالي**، ثم أنه المعالج لإتمام الاسترجاع.

6- يمكنك تحديد موقع الاسترجاع، وذلك بالنقر على زر **خيارات متقدمة** في الصفحة النهائية للمعالج.

هناك بعض النصائح عند عمل نسخ احتياطية هي:

- حاول أن تحفظ وسائط التخزين في مكان آمن، ويفضل أن يكون في مكان بعيد عن الحاسوب، حتى لا يتلف إذا تلف الحاسوب من جراء حريق أو غيره.
- تأكد من عمر وسائط التخزين الافتراضي.
- قم بالتخزين بشكل دوري.

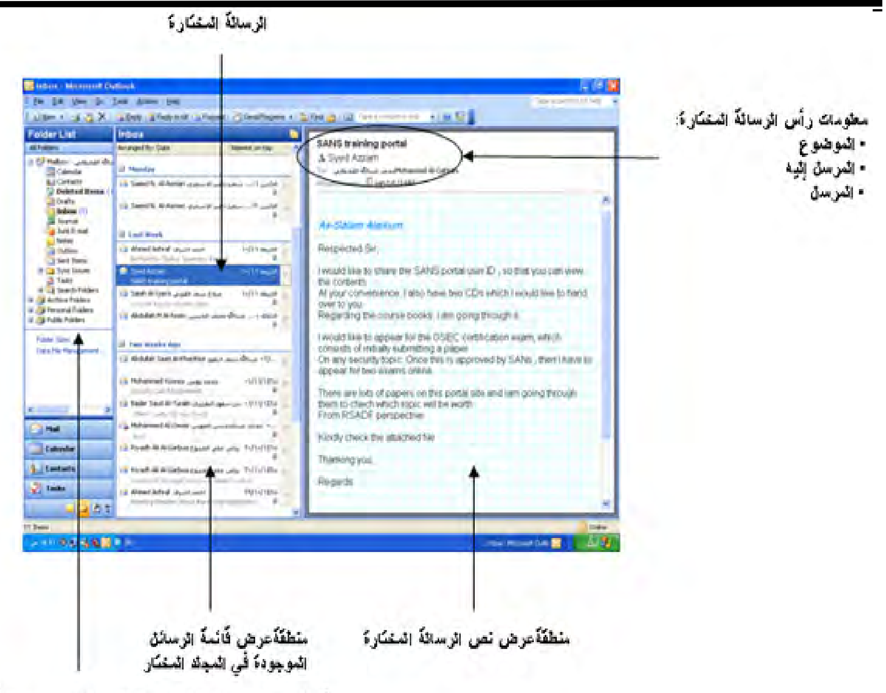
البريد الإلكتروني
E-Mail

تعد خدمة البريد الإلكتروني (E-mail) من أقدم الخدمات التي تقدمها شبكة الإنترنت. ويفترض أن معظم المستخدمين يعرفون كيف يستخدمون الخدمات الأساسية التي يقدمها البريد الإلكتروني، كإرسال الرسائل، واستقبالها، والرد عليها، ولكنْ قليلون هم أولئك الذين يعرفون الرحلة التي تقطعها الرسالة من نقطة الإرسال إلى وجهتها النهائية. وهذه المعرفة ضرورية لفهم طبيعة الأخطار التي تكتنف استخدام البريد الإلكتروني وحجمها، وبالتالي يمكن للمستخدم -فردا كان أو منشأة- أن يحدد ما يمكن إرساله، وما لا يمكن إرساله بواسطة البريد الإلكتروني، كما أن تجنب هذه الأخطار وغيرها يتطلب استخدام وسائل حماية -سنتطرق لبعضها لاحقاً-، ويتطلب كذلك فهماً لكيفية عمل البريد الإلكتروني، وهو ما سنحاول تبسيطه للقارئ.

إن أي مستخدم للبريد الإلكتروني لابد أن يتعامل مع ما يسمى برنامج البريد العميل، أو ما يسمى (E-mail client)، وهو البرنامج الذي يستخدم لإرسال الرسائل، واستقبالها، والرد عليها. وهناك نوعان رئيسان من هذا البرنامج:

(1) العميل القائم بذاته، مثل Outlook Express، وMicrosotf Outlook. وهذا البرنامج يسكن في حاسوبك الشخصي ويعمل هناك، والشكل (40) مثال على ذلك.

(2) العميل الذي يُعرض بواسطة المتصفح (Browser). ومن أمثلة هذا خدمة بريد ياهو (Yahoo)، وهوت ميل (Hotmail)، وهذا البرنامج لا يسكن في حاسوبك الشخصي، ولكن يسكن في مزودات خدمة عملاقة للشركة التي تقدم خدمة البريد مثل ياهو (Yahoo)، والشكل (41) يوضح ذلك.



الشكل (40): Micorsoft Outlook مثال لبرنامج بريد قائم بذاته.

وأياً ما كان نوع برنامج العميل المستخدم، فإنه يعمل الأشياء الآتية :

(1) عرض قائمة تشمل الرسائل الموجودة في صندوق بريد لـه، وهـذه القائمة تبين ما يسمى رأس الرسالة الذي يوضح اسم المرسل، وموضوع الرسالـة، وقـد يعرض أيضاً تاريخ الإرسال، وحجم الرسالة.

(2) تمكين المستخدم من اختيار رسالة ما، وقراءة محتواها.

(3) تمكـين المسـتخدم مـن إنشـاء رسـالة جديـدة، وكتابـة موضـوع للرسـالة (Subject)، وفحوى الرسالة (Message body)، ثم إرسالها إلى شخص، أو أكثر.

(4) اختيار ملفات معينة وإرسالها على شكل (Attachment) مع الرسالة ، كما يمكن صاحب البريد من حفظ المرفقات التي تصله مع الرسائل التي يستقبلها.



الشكل (41): واجهة بريد Yahoo الذي يعرض بواسطة المتصفح.

[1] كيف يعمل البريد الإلكتروني؟

إن البرنامج العميل لا يعمل بمفرده - و إن كان هو الشيء الوحيد الظاهر للعيان- بل إنه يستعين بخادم البريد الإلكتروني ، أو ما يعرف باسم (E-mail Server) الذي يتكون عادة من خادمين هما :

(أ) **بروتوكول (SMTP)**: مخصص لاستقبال الرسائل من المستخدمين المحليين ، وإرسالها إلى الوجهة المطلوبة ، كما يتصل بالخادمات الخارجية المماثلة لإرسال الرسائل

إليها، أو استقبال ما يخص المستخدمين المحليين من الرسائل الآتية من الخارج.

(ب) **بروتوكول (POP)**: يحفظ هذا البروتوكول الرسائل الواردة لكل مستخدم على حدة، ويساعد في عرضها عند الطلب. وهناك بروتوكولات أخرى يمكن استخدامها بدلا من (POP).

وسنعتمد على الشكل (41) لبيان كيفية عمل نظام البريد الإلكتروني. ففي حالة الإرسال يقوم المستخدم بإعداد الرسالة باستخدام أي برنامج عميل مثل (Microsoft Outlook)، ثم بعد الانتهاء يضغط زر الإرسال (الخطوة رقم 1 في الشكل). عندها يقوم بروتوكول (SMTP) باستقبال الرسالة (الخطوة رقم 2) التي يرسلها إلى وجهتها، وهناك احتمالان لا ثالث لهما هما:

* أن يكون مُصدر الرسالة والشخص الموجهة إليه مرتبطين بمزود خدمة بريد إلكتروني واحد. ففي هذه الحال يقوم بروتوكول (SMTP) بوضع الرسالة في الحيز المخصص للشخص الموجهة إليه (الخطوة ب).

* أن يكون مُصدر الرسالة والشخص الموجهة إليه مرتبطين بمزودي خدمة بريد إليكتروني مختلفين، وهنا يجري بروتوكول (SMTP) الذي يخدم مُصدر الرسالة اتصالا ببروتوكول (SMTP) المناظر له في مزود خدمة البريد الإلكتروني الذي يرتبط به الشخص الموجهة إليه الرسالة (الخطوة رقم 3)، ويبعث الرسالة إليه، أو يضع الرسالة في قائمة الرسائل المراد إرسالها (الخطوة رقم 4) إذا تعذر الإرسال لأي سبب، ثم يرسلها متى ما صار ذلك ممكنا (الخطوة رقم 5).

الشكل رقم (42): كيفية عمل نظام البريد الإلكتروني.

وحين تأتي رسالة مصدرها شخص مرتبط بمزود خدمة بريد إلكتروني آخر إلى مستخدم مرتبط بمزود خدمة البريد الإلكتروني المحلي (الخطوة أ) فإن بروتوكول (SMTP) يحفظ الرسالة الواردة في الحيز المخصص لذلك المستخدم (الخطوة ب). و عندما يفتح ذلك المستخدم برنامج البريد العميل فإنه يتصل مباشرة ببروتوكول (POP)، الذي يأخذ ما في حيز المستخدم من رسائل (الخطوة ج)، ثم يرسلها إلى برنامج البريد العميل (الخطوة د) ، فيعرضها الأخير.

[2] الأخطار التي تكتنف استعمال البريد الإلكتروني

يعد البريد الإليكتروني أكثر خدمات الإنترنت استعمالاً بين الشركات، والمؤسسات، وكذلك بين الأفراد، ويوجد ما يقارب 400 مليون صندوق بريد إلكتروني خاص بالشركات. أما عدد المستخدمين فقد شهد زيادة قدرها 20٪ سنوياً في العشرين سنة الماضية. وفي عام 2002م كان عدد الرسائل المتبادلة 14,9 بليون رسالة يومياً، أي قرابة 4 تريلون رسالة في العام، ويتوقع أن يصل عدد الرسائل المتبادلة عام 2005م إلى ما يقارب 35 بليون رسالة يومياً [1]. وهذه الأرقام لا تدل فقط على المراد ةاستعمال البريد الإلكتروني، فحسب، بل تدل كذلك على قوته بصفته أداة اتصال يمكن للشركات والأفراد استخدامها لمصلحتهم.

كما أن هذه الميزة ذاتها جعلت من البريد الإلكتروني، هدفا للهجمات الإلكترونية، ومن هذه الهجمات ما يلي:

(أ) استخدام البريد الإلكتروني لإغراق صناديق البريد الإلكتروني (E-mail account) – سواء الشخصية، أو تلك المملوكة للشركات– بالدعايات لمنتجات معينة. وفرز هذا البريد غير المرغوب فيه – الذي يسمى عادة (Spam) أو(Junk mail)، ويستهلك الموارد الحاسوبية للفرد أو المنشأة – يتطلب كثيراً من الوقت والمال، خاصة إذا عرفنا أن أكثر من نصف البريد الإلكتروني الذي تستقبله الشركات والمؤسسات هو من هذا النوع [2]. و قد يؤدي هذا النوع من الهجمات إلى خنق شبكات نقل المعلومات، مما يؤدي إلى حرمان مستخدمي أنظمة الحاسوب من تشغيل التطبيقات التي يحتاجونها، أو الوصول إلى شبكة الإنترنت.

---

(1) مقال بعنوان: "Controlling Unwanted Content" على موقع:
http://wstonline.bitpipe.com/data/detail?id=1097086148_820&type=RES&x=460943437

(2) المرجع السابق

(ب) إن البريد الإلكتروني كان – ولا يزال– وسيلة لنقل كثير من البرامج الخبيثة ونشرها.

(جـ) إضافة إلى ذلك فإن البريد الإلكتروني من الوسائل التي يستخدمها المهاجمون لجمع المعلومات الشخصية والمالية الحساسة، وهو ما يعرف باسم (Phishing scam)، أو ما يمكن أن نسميه بالنصب الإلكتروني باستخدام شبكة الإنترنت. ومن الأمثلة على ذلك أن يقوم المهاجم بإنشاء موقع على الإنترنت يشبه في مظهره الخارجي موقع شخصية اعتبارية مالية ذات أهمية للمستخدم، مثل البنك الذي يتعامل معه المستهدف، ثم ينتحل المهاجم شخصية البنك ويرسل إلى المستخدم بريدا إلكترونيا يطلب منه زيارة موقعه في الإنترنت لتحديث معلوماته الشخصية، لئلا يتعرض حسابه للإيقاف، ويعطي المستخدم رابطا إلى الموقع. وعند قيام المستخدم بالنقر على الرابط يأخذه ذلك الرابط إلى الموقع الذي أنشأه المهاجم. وبسبب شبهه بموقع البنك فإن المستهدف لا يدرك أنه قد استدرج، ثم يطلب الموقع منه أن يدخل بياناته الحساسة، مثل: رقم حسابه، ورقمه السري وغيرها، ثم يخرج من الموقع دون أن يكتشف أنه كان ضحية نصب إلكتروني. ومن المؤشرات على انتشار النصب الإلكتروني أن الخسائر جراء هذا النوع من النصب ارتفعت من 3،262،834 دولارا في عام 1999م إلى 14،647،933 دولارا في عام 2002م، أي بزيادة قدرها 448٪ في غضون أربع سنوات فقط[1]. ومن المؤشرات كذلك أن شركة F-Secure سمت عام 2004م عام النصب الإلكتروني[2].

---

(1) مقال بعنوان: "What it is, how can it affect us, and how to deal with spam." على موقع: http://www.sans.org/rr/whitepapers/email/1111.php

(2) مقال بعنوان: "F-Secure Corporation's Data Security Summary for 200" على موقع: http://f-secure.com/2004

وتشير بعض التقارير إلى أنه في سنة 2004م كان البريد غير المرغوب فيه يمثل 70٪ من البريد الذي يصل إلى المستخدمين. وتقدر التكاليف التي لحقت بالشركات عام2003م نتيجة البريد غير المرغوب فيه بألفي دولار لكل موظف بالشركة[1].

ولدرء هذه الأخطار وغيرها ظهر ما يسمى فرز البريد الإلكتروني، وهو ما نتحدث عنه في الفصل التالي.

[3] فرز البريد الإلكتروني (E-mail Filtering)

يقصد بفرز البريد الإلكتروني التخلص من البريد غير المرغوب فيه (Spam). وتمكن التقنيات المتاحة اليوم إجراء عملية الفرز في موضعين:

(أ) برنامج عميل البريد الإلكتروني (Client E-Mail): يمرر جميع البريد القادم إلى برنامج عميل البريد الإلكتروني، حيث تجري عملية الفرز هناك. وتتميز هذه الطريقة بسهولتها، وأنها تعطي المستخدم قرار تحديد ما يعتبر مرغوباً وما ليس مرغوباً. لكن لهذه الطريقة عيوب منها: أن البريد غير المرغوب فيه يجب أن ينقل إلى برنامج العميل قبل تصفيته، وهذا البريد قد يكون كبير الحجم، مما يسبب اختناق الشبكة، كما أن نقله يستغرق وقتاً طويلاً، خاصة إذا كانت وسيلة ربط المستخدم بشبكة الإنترنت بطيئة كخط الهاتف، مثلاً، ومن عيوب هذه الطريقة أيضا أنها لكي تعمل بصورة صحيحة، فإنه يجب أن تكون جميع الحواسيب مزودة بالبرامج المضادة للفيروسات (Antivirus)، وإلا اخترقت الفيروسات تلك الأجهزة، وتحميل جميع الأجهزة بالبرامج المضادة للفيروسات وتحديث تلك البرامج باستمرار يعد أمراً صعباً، بل قد يكون أقرب إلى المستحيل إذا فكرنا في تحميلها في جميع الأجهزة المرتبطة بمزود خدمة الإنترنت (ISP)، مثلاً.

---

(4) مقال بعنوان: "Spam Classification Techniques" على موقع:
http://searchwindowssecurity.techtarget.com/whitepaperPage/0,293857sid45_gci1010912,00.html

(ب) مزود خدمة البريد الإلكتروني(Server E-Mail): في هذه الحالة تتركز جهود الفرز في مزود الخدمة نفسه، وهذه الطريقة هي السائدة حالياً، مع إعطاء المستخدم بعض القدرات على الفرز.

وهناك عدة طرق لفرز البريد الإلكتروني، غير أن أيًّا منها لا يكفي منفرداً لحل معضلة البريد غير المرغوب فيه. وتبعاً لذلك فإنه ينصح بتطبيق أكثر من طريقة للحد من آثار هذه المعضلة. ومن أشهر الطرق الآتي:

أ- طريقة القائمة السوداء (Black List): تعتمد هذه الطريقة على تكوين قائمة سوداء توضع فيها العناوين الرقمية للجهات التي ترسل البريد غير المرغوب فيه، فكلما جاءت رسالة جديدة يقوم مزود خدمة البريد الإلكتروني بالتأكد من أن مصدر الرسالة ليس ضمن القائمة السوداء، فإن كان ضمنها فإن الرسالة تحذف، وإن لم يكن فإن الرسالة تعد بريداً مرغوباً فيه. لكن إذا اكتشف لاحقاً أن الرسالة هي في حقيقتها بريد غير مرغوب فيه فإن مرسلها يضاف إلى القائمة السوداء. ويتولى إداري الشبكة تحديث هذه القائمة السوداء ومتابعتها. وقد حسنت هذه الطريقة بحيث يمكن للجهات المختلفة التعاون بينها لتوحيد جهودها لتكوين قائمة سوداء مشتركة. لكن من عيوب هذه الطريقة أن مرسلي البريد غير المرغوب فيه يستخدمون آلافاً من العناوين، كما أنهم يزورون عناوينهم، ولذلك فإن متابعة كل هذه العناوين أمر مكلف وغير فعال.

ب- طريقة القائمة البيضاء (White List): هذه الطريقة تستخدم المنطق المعاكس لسابقتها، فيفترض هنا أن كل رسالة هي بريد غير مرغوب فيه ما لم يكن المرسل في القائمة البيضاء التي تضم المرسلين المسموح استقبال البريد الآتي من قبلهم، ومع أن هذه الطريقة توفر قدراً كبير من الحماية ضد البريد غير المرغوب فيه، فإنها

قد تمنع وصول بريد مرغوب فيه، إذا كان قادماً من جهة ليست في القائمة البيضاء.

جـ ـ طريقة محركات القواعد المساعدة (Heuristics Engines) :

تعتمد هذه الطريقة على مجموعة من القواعد التي يضعها المختصون لتحديد ما إذا كانت رسالة ما بريداً غير مرغوب فيه، ثم توضع هذه القواعد في محرك على صورة برنامج يقوم بعمل الفرز آلياً. وبصورة مبسطة يمكن القول إن هذه القواعد تقوم على البحث عن خصائص وصفات يغلب وجودها في البريد غير المرغوب فيه. فمثلاً يكثر في البريد غير المرغوب فيه تقديم عروض مجانية، أو الوعود بالحصول على ثروة، أو لقطات جنسية؛ وذلك لأن مرسلي البريد غير المرغوب فيه غالباً ما يراهنون على ما يثير المستخدم. ويحاول مرسلو البريد الإلكتروني إيجاد طرق للالتفاف على البرامج التي توفر الحماية بطريقة القواعد المساعدة. ومن عيوب هذه الطريقة الحاجة المستمرة لتحديث القواعد.

د- طريقة التصنيف المبني على إحصاءات: عند استخدام هذه الطريقة تجمع معلومات من البريد غير المرغوب فيه الذي يرد إلى الجهة التي تستخدم هذه الطريقة. وهذه المعلومات تشمل البحث عن الكلمات الواردة في خانة موضوع الرسالة أو نصها الأصلي، وبناء على المعلومات التي تم جمعها من البريد غير المرغوب فيه تعد إحصاءات تستخدم لاحقاً عند قدوم رسائل جديدة في تحديد احتمال أن تكون هذه الرسالة بريداً غير مرغوب فيه، وذلك بالبحث عن الكلمات الواردة في خانة الموضوع، أو نص الرسالة. وتمتاز هذه الطريقة بدقتها الفائقة، وأنها لا تحتاج إلى تحديث مستمر من قبل المشرف على الشبكة.

[4] أفضل طرق التعامل مع البريد الإلكتروني

(أ) تجنب استخدام البريد الإلكتروني لإرسال المعلومات الحساسة، كرقم بطاقة الائتمان، أو رقم حسابك في البنك، أو كلمة المرور ..إلخ ما لم يكن البريد الإلكتروني الذي تستخدمه مشفراً. ومن حيث الأصل فإن رسائل البريد الإلكتروني ترسل على هيئة

نص غير مشفر يمكن لأي إنسان قراءتها، وعند الرغبة في تشفير البريد الإلكتروني لابد من شراء برامج خاصة لهذا الغرض مثل برنامج (PGP).

(ب) تجنب إرسال الملفات الكبيرة جداً كمرفقات البريد الإلكتروني (Attachment)، وذلك لأن مزود خدمة البريد الإلكتروني مصمم للتعامل بفعالية مع الرسائل التي ليست لها مرفقات، وكذلك الرسائل التي معها مرفقات تتراوح بين صغيرة ومتوسطة الحجم. وعندما ترسل الملفات الكبيرة فإنها تسبب اختناقات في الشبكة بسبب بطء مزودات الخدمة في التعامل مع هذه الملفات. وهناك وسائل بديلة لإرسال الملفات الكبيرة جداً، مثل برنامج (FTP) الخاص بنقل الملفات الكبيرة جداً.

(جـ) تأكد من خلو الرسائل التي ترسلها من أي أوجه شبه بالرسائل غير المرغوب فيها، وإلا فإن رسائلك قد تتعرض للحذف من قبل أنظمة فرز البريد الإلكتروني لدى المستقبل.

(د) وضع الغرض من الرسالة في خانة الموضوع من الرسالة التي تعدها، ويمكن أن توضح اسم الجهة التي ترسل منها لإعطاء الرسالة قدراً أكبر من الموثوقية.

(هـ) حافظ على عنوانك الإلكتروني (Email address)، فلا تعط عنوانك إلا لمن تثق به.

(و) لا تفتح المرفقات القادمة من أشخاص لا تعرفهم، وكذلك لا تفتح المرفقات القادمة من أشخاص تعرفهم إذا لم يكن إرسالها متوقعاً.

(ز) إذا كنت تتوقع وصول بريد إلكتروني من أشخاص تعرفهم، وتتوقع كذلك وصول مرفقات فقبل فتح المرفقات تأكد من فحصها باستخدام نظام كشف الفيروسات.

(حـ) ابق نظام كشف الفيروسات محدثاً في جهازك.

(ط) بعـض أنظمـة البريـد الإلكترونـي تعطـي خاصـية التحميـل التلقـائي (Automatic Download) للمرفقات، عليك أن توقف تشغيل هذه الخاصية.

(ي) عندما تستقبل بريداً غير مرغوب فيه فيمكنك إعلام برنامج عميل البريد الإلكتروني بأن هذا البريد غير مرغوب فيه، وبالتالي يقوم البرنامج بحجب ذلك البريد مستقبلاً.

[5] طرق مقترحة لحماية البريد الإلكتروني

(أ) بروتوكول (S/MIME) للبريد(1): يعتمد هذا البروتوكول على نظام تشفير معين يمكنه من تقديم خدمتين أساسيتين:

(1) الحفاظ على سرية الرسائل.

(2) الحفاظ على سلامة الرسائل.

ولكي يعمل البروتوكول لابد من الآتي:

(1) أن يكون لدى كل مستخدم مفاتيح التشفير اللازمة.

(2) أن يكون لدى كل مستخدم شهادة مصادق عليها من جهة معتمدة، بحيث يمكن لأي من المتعاملين بهذا البروتوكول التحقق من هوية من يتعامل معه بالتحقق من الشهادة التي يبرزها. وهذه الشهادة محفوظة في شكل رقمي بحيث يمكن إرسالها عبر شبكة المعلومات عند الحاجة.

(3) أن يكون برنامج عميل البريد الإلكتروني في الجهاز الخاص بالمستخدم فيه خاصية التعامل مع بروتوكول (S/MIME)، فبرنامج (Microsoft Outlook Express) و(Office Outlook)، والنسخة 7 من برنامج (Netscape Messenger) يمكنها التعامل مع (S/MIME).

(ب) بروتوكول (PGP): يعتمد هذا البروتوكول على مزيج مؤلف من أنظمة

---

(1) http://www.dartmouth.edu/~pkilab/pages/Using_SMIME_e-mail.html

التشفير، وقد قامت عدة شركات بتطوير تطبيقات معتمدة في أساسها النظري على هذا البروتوكول، ومن المواقع الشهيرة التي يمكن تحميل هذه التطبيقات منها موقع http://www.pgp.com/ . وتتفاوت هذه التطبيقات في مقدار الخدمات التي تقدمها، ولكنها عموما تقدم خدمة تشفير البريد الإلكتروني أثناء إرساله، و بعضها يزيد على ذلك بتشفير الرسائل أثناء تخزينها في الحاسوب.

الخلاصة

البريد الإلكتروني – كالمشاركة في الملفات – إحدى وسائل تسهيل العمل وزيادة الإنتاج، ولكنها في الوقت ذاته تفتح ثغرات أمنية في منظومة المعلومات، ولذلك لابد أن يتعرف المستخدم على الطريقة الصحيحة للاستفادة من هذه الوسيلة، وتوقي أخطارها. لكن بعض جوانب الحماية من البريد الإلكتروني يتطلب معرفة تقنية أكثر عمقا من تلك المطلوبة للمشاركة في الملفات، ولا بد من إيكال هذه المهمة للمتخصصين في أمن المعلومات. ولكن هذا لا يعني، بحال، أن المستخدم ليس له دور يلعبه، بل إن دوره مكمل لدور المتخصصين، وقد مر بنا عدد من الإجراءات التي يمكن للمستخدم العادي اتباعها لتقليل الأخطار المصاحبة لاستخدام البريد الإلكتروني.

التســوق الآمـــن
Secure Online Shopping

لقد كان ضرباً من الخيال التسوق دون الذهاب للسوق، أو ما يعرف بالتسوق بلبس البيجاما! لكن الآن مع وجود خدمة الإنترنت بات بالإمكان التسوق من البيت، ليس فقط في المتاجر المحلية (بافتراض أن المحلات لديها موقع على الإنترنت)، بل و أيضاً في المتاجر العالمية. لكن حتى مع ما قدمته هذه النقلة النوعية من سهولة ويسر وتنوع في عملية التسوق فإن أخطارها أكثر من عملية التسوق التقليدي، ونأخذ بعض الفروق :

	التسوق التقليدي	**التسوق بواسطة الإنترنت**
مكان المتجر	معروف ومحسوس	غير محسوس
معرفة المتجر لاسمك	ليس بالضرورة	يعرف
معرفة المتجر لعنوانك البريدي	ليس بالضرورة	يعرف
معرفة المتجر لمشترياتك السابقة	ليس بالضرورة	يعرف
معرفة المتجر لمعلومات بطاقتك الائتمانية	لا يعرف إذا قمت بالدفع بالنقود	يعرف حيث إن أغلب المتاجر تطلب الدفع بالبطاقة الائتمانية
تكشف معلوماتك نتيجة الشراء من المتجر	ليس بالضرورة	نعم
تعرض شخصيتك للانتحال	صعبة	سهلة
تعرض معلوماتك للبيع لشركات أخرى بدون علمك	لا	نعم

نخلص إلى القول إن التسوق ـ[illegible] لإنترنت محفوف بالأخطار الأمنية،

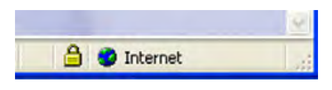
وأكثر عرضة لانتهاك الخصوصية، لذا لابد من الحرص أثناء التسوق عن طريق الإنترنت واتباع التعليمات التالية:

* كما هو معلوم فإن الإنترنت غير مشفرة، ويمكن لمن يتصنت على الإرسال أن يعرف فحوى المرسَل والمستقبَل، أي عند إرسالك لمعلوماتك الشخصية بما فيها معلومات بطاقتك الائتمانية عن طرق البريد الإلكتروني غير المشفر، أو أحد مواقع الإنترنت، فأنت تعرض معلوماتك للغير بكل وضوح. لكن هناك تقنيات تستخدمها المتاجر لتشفير معلوماتك المهمة وحمايتها عند انتقالها منك إليهم. ولمعرفة ما إذا كان الموقع أو المتجر يقوم بتشفير معلوماتك أثناء انتقالها يمكنك بكل بساطة، معرفة ذلك عند ملء المعلومات، وذلك بالتحقق من أمرين:

* إن عنوان الصفحة التي تطلب المعلومات يبدأ بـ: https، وليس http، لاحظ وجود حرف S بعد http.

موقع مشفر	https://www.amazon.com
موقع غير مشفر	http://www.amazon.com

* وجود صورة قفل في الشريط السفلي لمتصفح الإنترنت في المعلومات، كما في الشكل (43):



الشكل رقم (43): قفل الحماية.

* استخدم كلمة مرور مختلفة عن تلك الخاصة بالدخول للنظام أو البريد الإلكتروني؛ لأنه في حالة معرفة أحد المهاجمين لكلمة المرور الخاصة بك في المتجر، فإنه يستطيع الوصول لنظامك أو بريدك الإلكتروني، كما يقول المثل "لا تضع جميع

بيضك في سلة واحدة".

* استخدم بطاقة ائتمان واحدة خاصة بالتسوق عبر الإنترنت.

* إذا كان الخيار لك، فلا تسمح بتخزين معلومات بطاقة الائتمان في المتجر؛ لأنه قد يُخترق الموقع الإلكتروني للمتجر، وتُسرق جميع بطاقات الائتمان؛ خاصة إذا كانت الإجراءات الأمنية للمتجر غير متينة. ونحن نسمع بين الفينة والأخرى عن سرقة أحد المهاجمين لقاعدة بيانات بطاقات الائتمان لعملاء متجر معين. وفي تلك الحال يتوجب على المتجر إبلاغ جميع العملاء عن تلك الحادثة، واستبدال أرقام جديدة ببطاقاتهم، وفي حال فقدانك لبطاقتك فإنه يتوجب عليك سرعة الإبلاغ عن السرقة وإيقاف البطاقة. لاحظ أن البطاقة ما زالت لديك وبمحفظتك، لكن معلوماتها (الاسم، الرقم، تاريخ الانتهاء، عنوان السداد) سرقت، ويمكن استخدام تلك المعلومات للشراء دون الحصول على البطاقة الفعلية.

* لا تخزّن معلوماتك في الجهاز، خاصة كلمة المرور، ومعلومات بطاقة الائتمان.

* تعامل مع متاجر معروفة.

* اطبع أو احفظ إلكترونياً عمليات الشراء عن طريق الإنترنت للرجوع إليها عند الحاجة.

* توخ الحذر عند كتابة اسم الموقع، فهناك مواقع تستغل خطأ الزائر في أحد حروف اسم الموقع المطلوب لشده و الحصول على معلومات سرية عنه. فبدل أن تكتب: http://www.hotmail.com كتبت: http://www.hutmail.com.

* حدث برنامج المتصفح، ونظام التشغيل (ويندوز) بشكل دوري لتفادي أي

ثغرات أمنية قد تؤدي إلى اختراق المتصفح.

* تأكد من عمل برنامج مكافحة الفيروسات وتحديثه بشكل دوري.

الخلاصــة

إن التسوق عن طريق الإنترنت محفوف بالأخطار الأمنية ، وأكثر عرضة لانتهاك الخصوصية ، و على من يريد التسوق تذكر أن هناك من يتربص به. لذا لابد من توخي الحذر أثناء التسوق عن طريق الإنترنت ، واتباع توصيات الأمان التي عرضنا طرفا منها.

السرية على الإنترنت

التسوق على الإنترنت، وكذلك التصفح يعرض معلومات للاطلاع من قبل الغير؛ فعند الشراء يسجل معلوماتك؛ وعند التصفح يسجل تحركاتك. لذلك لابد من الحذر من إعطاء المعلومات، فقد تبدو لك معلومة أنها بسيطة، لكن إذا جمعت مع معلومات أخرى قد تكون مهمة.

للحفاظ على سرية معلوماتك -قدر الإمكان- قم بالتالي:

* اقرأ سياسة "سرية المعلومات" للمتجر. فإذا كان المتجر مرموقاً فإنه لابد من أن يوضح سياسة المتجر عن سرية معلومات العميل، والسياسة تبين التالي:

* ما هي المعلومات التي يجمعها المتجر من العميل. فقد تفاجأ بحصول المتجر على معلومات لم تظن أنه قد يحصل عليها.

* كيفية استخدام المتجر لتلك المعلومات، وبعض المتاجر قد تبيع المعلومات لمتاجر أخرى، أو شركات إعلانية.

* معرفة مدى مقدرتك على تفادي المعلومات أو نشرها. فبعض المتاجر تتيح لك خيار نشر المعلومات، فاستفد منها قدر الإمكان.

* لا تقدم معلومات غير مطلوبة، أو تظن أنها لا علاقة لها بالشراء، كرقم بطاقة الأحوال (مثلاً).

* لا تقدم معلومات خاصة لجهات أو أشخاص غير معروفين.



الشكل رقم (44): خيارات إعداد برنامج متصفح الإنترنت.

* عند استخدام حاسوب عمومي كالذي في مقاهي الإنترنت، بل ولتلافي كشف معلوماتك الشخصية في جهازك لأي مهاجم محتمل، احرص على حذف معلومات تصفحك. ويمكنك فعل ذلك عبر الخطوات التالية:

* **أولاً**: تحت قائمة: **أدوات | خيارات إنترنت**، ثم تحت صفحة "عام" قم بالنقر

على زري "حذف ملفات تعريف الارتباط"، و زر "حذف ملفات..."، كما في الشكل (44).

* **ثانياً** : تحت قائمة : **أدوات | خيارات إنترنت**، ثم تحت صفحة "**محتـــوى**" انقر على زر "**إكمـــال تلقـــائي**"، ثـم زري : "مسح كلمات المرور"، و زر "مسح النماذج"، كما في الشكل(45).



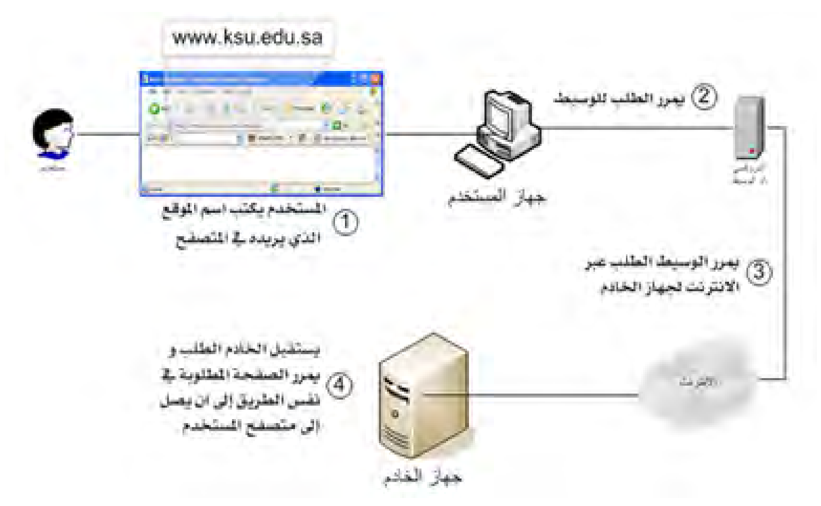
الشكل رقم (45): إعدادات الإكمال التلقائي.

الخلاصة

الحفـاظ علـى سـرية معلومـات المسـتخدم هـي في المقـام الأول مسـؤوليته الشخصية، و على المرء أن يتذكر أن المعلومات المتفرقة قد لا تكون ذات قيمة، و لكنها إذا اجتمعت تصبح ذات قيمة بالغة.

متصفح ميكروسوفت للإنترنت
Microsoft Internet Explorer

شبكة الإنترنت هي مجموعة حواسيب متصلة بعضها ببعض. وهناك نوعان من الحواسيب على شبكة الإنترنت: حواسيب خادمة، وهي التي تقوم بتقديم المعلومات والخدمات للحواسيب الأخرى التي تسمى الحواسيب المستفيدة، وهي النوع الثاني. أمّا الشبكة العنكبوتية العالمية، أو ما يعرف بمصطلح (www) فهي حواسيب خادمة تقدم معلومات للمستفيدين بصيغة محددة، والصيغة معتمدة على لغة الترميز المتشعب (HTML).



الشكل رقم (46): طريقة تصفح الانترنت.

بوابتك على الإنترنت تبدأ من متصفح الإنترنت الذي من خلاله يمكنك قراءة الصفحات، والتسوق، والمحادثات، وتنزيل الملفات المختلفة، وكذلك إدارة حساباتك المختلفة، ومن ضمنها حسابك البنكي الخاص. والمتصفح برنامج يقرأ المعلومات التي

كتبت بلغة الترميز المتشعب، ثم يقوم بترجمتها إلى نص وأشكال كما أرادها مصمم الصفحة. والوصول إلى الموقع المطلوب عن طريق المتصفح يمكن تمثيله بشكل (46).

نظراً لشعبية متصفح ميكروسوفت للإنترنت، فإننا سوف نركز على هذا النوع من المتصفحات مع أن المهاجمين يتهافتون على مهاجمته أكثر من غيره من المتصفحات.

[1] تحصين المتصفح

قلنا إن المتصفح هو بوابتك إلى الشبكة العنكبوتية العالمية، فإذا تخيلت أن تلك البوابة بوابة قلعة مهمة يدخل منها ويخرج الناس والبضائع، ماذا سوف تعمل؟ بالطبع سوف تعمل جاهداً على تحصين تلك البوابة ووضع الأنظمة والقواعد (الإعدادات الأمنية) للسماح بالخروج وبالدخول، ومتصفح الإنترنت لا يصح أن يكون أقل أهمية من بوابة القلعة.

يزيد تحصين البوابة من مقاومتها للهجمات. فبوابة القلعة تُفحص بشكل دوري للتأكد من صلابتها وخلوها من أي شقوق أو فتحات؛ وعند اكتشاف أي خلل أو عيب قد يقلل من مهمة البوابة، فإن الخلل أو العيب يُزال بشكل عاجل. وكذلك يجب أن يُتعامل مع بوابة الإنترنت وهي متصفح الإنترنت.

وعملية تحصين متصفح الإنترنت أسهل بكثير من تحصين بوابة القلعة، وتكمن عملية تحصين متصفح الإنترنت في التأكد من أن جميع التحديثات الأمنية الجديدة للمتصفح تم إضافتها للمتصفح، والتحديثات الأمنية هي تحسينات للمتصفح لسد أي ثغرات أمنية مكتشفة قد تؤدي إلى ضعف المتصفح وتعريته أمام المهاجمين. وكثيراً ما تنتشر الفيروسات، والديدان الضارة باستغلال ثغرة أمنية لم تُسد، مع العلم أن علاج الثغرة يكون غالباً متاحاً للمستخدم.

إن عملية تحصين متصفح ميكروسوفت سهلة للغاية. ما عليك إلا الذهاب إلى صفحة تحديثات الويندوز على موقع شركة ميكروسوفت، الذي بدوره يفحص

المتصفح وغيره من برامج ميكروسوفت، ويتأكد من تثبيت جميع التحديثات الحديثة، يمكنك مراجعة ..(رقم الفصل).... في هذا الكتاب للحصول على معلومات أكثر عن تحديث الويندوز.

[2] اللغات الحديثة للمتصفح

قبل أن نتحدث عن الإعدادات الأمنية للمتصفح يجب أن نتطرق إلى بعض اللغات المهمة التي قد تستخدم في المتصفح، والتي قد تؤدي إلى خروقات أمنية. فكما قلنا سابقاً إن لغة الترميز المتشعب (HTML) هي اللغة الأكثر انتشاراً لترميز صفحات الإنترنت، لكن هذه اللغة تفتقر إلى الخصائص اللازمة لتكوين محتوى متغير (Dynamic Content) لكل مستخدم ولكل وقت، مثل: عرض درجة حرارة مدينتك، لذلك أضيفت لغات جديدة لهذا الغرض، من أمثلتها: والتي سوف نتحدث عنها، وعن المشاكل الأمنية المتعلقة بتلك اللغات:

.JavaScript, Java Applet, ActiveX

شفرة الجافا **Java Script**

تعتمد على لغة جافا المشهورة، ولكنها مخصوصة للعمل مع لغة الترميز المتشعب (HTML) لغرض التحكم في المتصفح وفي تهيئته، وفتح النوافذ وغلقها، وتحميل بريمجات جافا وتنزيلها وتنفيذها لأغراض محدودة، وفي نطاق ضيق جداً. لكن لوجود ثغرات أمنية في بعض المتصفحات يمكن لبرنامج مكتوب بلغة JavaScript أن يقوم بأعمال خبيثة دون علم المستخدم، كأن يقرأ ملفات خاصة، أو يراقب عمل المستخدم، والمواقع التي يزورها، أو أن يستخدم حساب بريد المستخدم لإرسال رسائل زائفة. لذلك يجب عليك تحديث برنامج المتصفح، وتفادي زيارة المواقع المشبوهة. وإذا أردت أمانا أكثر، عطل عمل Java Script ، لكن هذا الإجراء قد يؤثر في

عمل بعض الصفحات التي تعتمد على Java Script. ويمكنك الوصول إلى منطقة تعديل هذا الخيار، كما في الشكل (47).

بريمج الجافا Java Applet

يعد برنامج Java Applet ، أو ما يعرف ببريمج الجافا نوعاً متفوقاً عن Java Script ، ويتميز باستقلاليته عن صفحة لغة الترميز المتشعب (HTML)، ويقدم خصائص متقدمة لعمل الحسابات والرسومات بدون الرجوع للحاسوب الخادم. وبريمج الجافا يمكن أن يُستغل استغلالاً غير مشروع، بحيث يمكن أن يصل إلى ملفات النظام وعمل فعل خبيث، كحذف ملفات أو تحميل فيروس. ولحل تلك الأعمال غير المشروعة استحدث ما يسمى صندوق الرمل (Sandbox) الذي يحد من إمكانيات بريمج الجافا بوضع حواجز حول البريمج لمنعه من الوصول إلى ملفات المستخدم والتحكم بالنظام. لكن للأسف لم يكن الحاجز كافياً لمنع الاختراقات، فقد تم اختراقه.

هناك نوعان من بريمجات الجافا هما:

1) بريمجات الجافا الموقعة، و هي التي تأتي من مصدر موثوق ولم يتم تعديلها.

2) بريمجات الجافا غير الموقعة، والتي لم تأت من مصدر موثوق أو معدلة، والبريمجات غير الموقعة تعمل داخل صندوق الرمل، ومحدودة، بعكس البريمجات الموقعة تكون غير محدودة، إذا أرادت إحدى البريمجات الخروج خارج صندوق الرمل، فإنه ينتج عنه إنذار للمستخدم يبين له أنه ليس بريمجاً موقعاً.

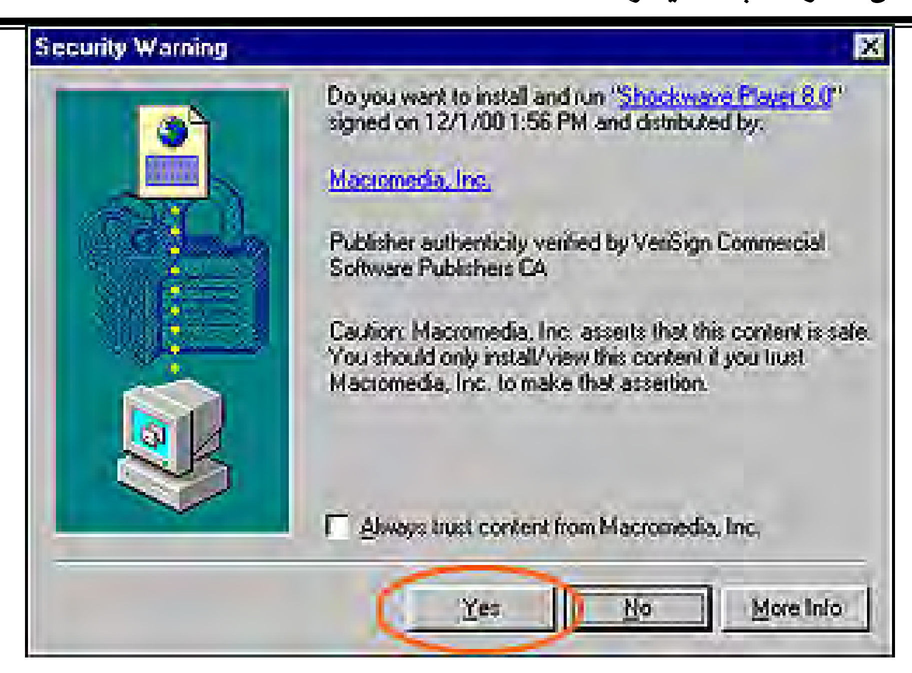
وللحصول على مستوى أمني مرتفع، لا تقبل بعمل أي بريمج جافا غير موقع إلا إذا تأكدت من مصدره. ويمكنك الوصول إلى منطقة تعديل هذا الخيار كما في الشكل (47).



الشكل رقم (**47**): خيارات بريمجات الجافا.

بريمجات الأكتف إكس (ActiveX Controls)

تقنية متقدمة من شركة ميكروسوفت لتوزيع البرامج عبر الإنترنت، ولربط مكونات التطبيقات المختلفة مثل عرض تطبيقات ميكروسوفت أوفيس (Microsoft Office) على الإنترنت. وبريمجات الأكتف إكس قد تتيح للمبرمج تنفيذ أي عملية على جهاز المستفيد. وأمان هذه البريمجات يعتمد على الثقة في الجهة المنتجة لها. فعند الدخول لموقع يستخدم هذه البريمجات يسألك المتصفح عمّا إذا أردت الوثوق في الجهة المنتجة، والسماح لعمليات البريمج بالعمل، لكن هذا السؤال يُسأل فقط في أول استخدام للبريمجات. وقد لا يعير المستخدم السؤال الموجه إليه عن هذه البريمجات أي أهمية، وينتج عن ذلك تعرضه للهجوم. ولنأخذ هذا السيناريو: زرت موقعاً مشبوهاً



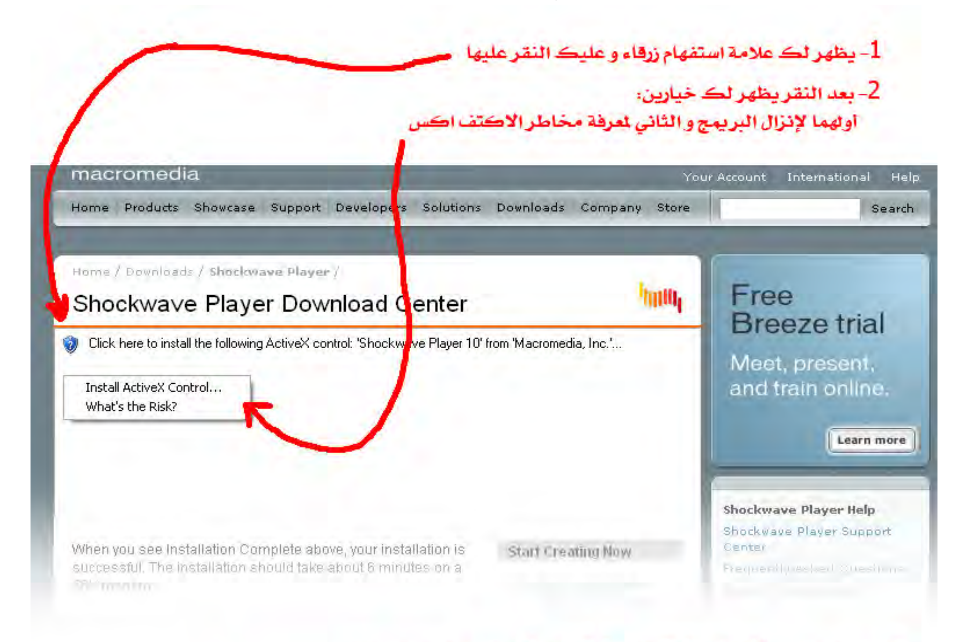
الشكل رقم (**48**): شاشة الموافقة على تحميل بريمج أكتف إكس.

لإنزال برنامج غير قانوني، لكن الموقع اشترط عليك لكي ينزل البرنامج أن توافق على السؤال الموجه إليك ليتسنى لـه إنزال البرنامج في جهازك (طبعاً هذا غير صحيح)، وأنت بلا مبالاة، أو دون علم بأضرار السؤال الجانبية وافقت. لقد أعطيت في هذه الحالة لصاحب الموقع الضوء الأخضر لعمل ما يبدو له في جهازك من قراءة ملفاتك، أو إنزال برامج خبيثة تجسسية فيه، أو وضع جهازك عبداً لـه لتنفيذ هجمات على أجهزة أخرى من جهازك الذي أنت مسؤول عنه أولاً وأخيراً. ينبغي حينئذٍ الحذر من بريمجات الأكتف إكس، والتأكد من المصدر لتلك البريمجات.

عندما تُسأل عن الموافقة على إنزال بريمج أكتف إكس يكون شكلها مثل: شكل (48).

لكن مع التحديث الأمني مع حزمة SP2 لويندوز XP تغيرت طريقة إنزال بريمج

أكتف إكس قليلاً، فأصبحت كالتالي :



3- بعد النقر على "Install ActiveX Control" يظهر لك الشكل التالي



الشكل رقم (49): تحميل بريمج اكتف إكس.

(4) الشكل (49) يبين اسم البريمج وناشره، ويسألك عن:

1- دائماً تنزل برامج من هذا الناشر.

2- لا تنزل برامج من هذا الناشر أبداً.

3- اسألني كل مرة.

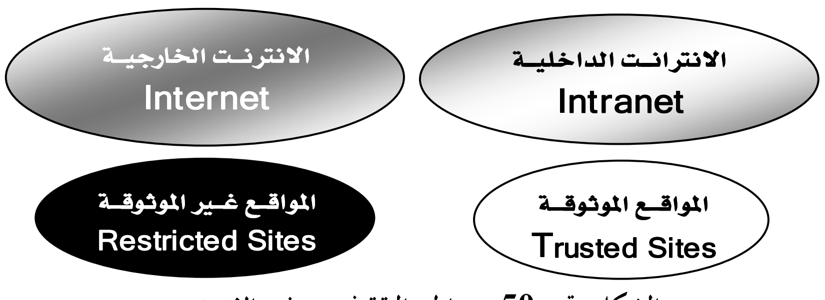
ثم لك الخيار في قبول إنزال البريمج.

وللحصول على مستوى أمني مرتفع عليك بتعطيل بريمجات الأكتف إكس، ولكن يترتب على هذا الاستغناء عن خدمات بعض المواقع، ويمكنك الوصول إلى منطقة تعديل هذا الخيار كما في الشكل:

[3] الإعدادات الأمنية للمتصفح

أ- المناطق الأمنية

المتصفح بوابتك لمنطقتين: الإنترنت الداخلية (الشبكة الداخلية للمنظمة أو البيت)، والإنترنت الخارجية (كل موقع خارج المنظمة أو البيت). إن معرفة هاتين المنطقتين مهم لإدارة الجوانب الأمنية، وبالتحديد الجوانب الأمنية في متصفح الإنترنت. ولتوضيح التصور من متصفح الإنترنت وتقريبه هناك أيضا منطقتان، أو بالأحرى قائمتان هما المواقع الموثوقة والمواقع غير الموثوقة، ومتصفح الإنترنت يتعامل مع أربع مناطق كما في شكل رقم (50).



الشكل رقم (50): مناطق الثقة في متصفح الانترنت.

ب- الإنترنت الداخلية

هي عبارة عن:

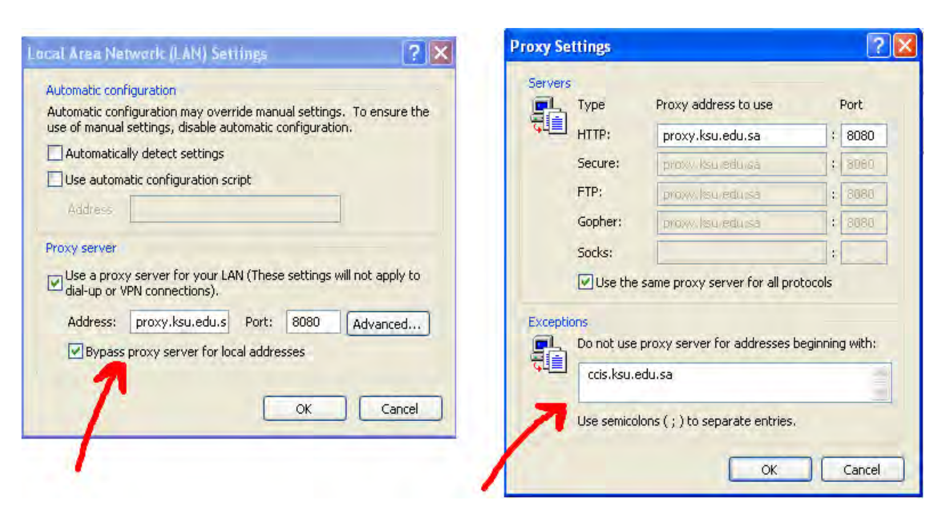
* جميع المواقع الداخلية للمنظمة أو البيت.

* المواقع التي بهيئة Universal Naming Convention (UNC) التسـمية المتفقة العالمية.

مثل :

\\server-name\shared-resource-pathname

* المواقع التي تتخطى جهاز البروكسي أو الوسيط ، ولا تحتاج إليه ، والتي تم تحديدها بواسطة كتابتها في إعدادات المتصفح كما في الشكل (51).



الشكل رقم (51): المواقع التي تتخطى جهاز البروكسي أو الوسيط.

جـ- الإنترنت الخارجية

جميع المواقع خارج المنظمة وليسو من ضمن المواقع الداخلية ، أو الموثوقة ، أو غير الموثوقة.

*** المواقع الموثوقة**

جميع المواقع التي حددها المستخدم على أنها موثوقة. يتم ذلك بواسطة :

أدوات | إعدادات إنترنت | أمان | المواقع الموثوقة ، كما في الشكل

(52)، ثم النقر على زر مواقع، ثم إضافة الموقع الذي تود إضافته للمواقع الموثوقة.

لاحظ أن المتصفح يُلزمك بإدخال مواقع مشفرة الاتصال، و تبدأ بصيغة https:\\، لكن يمكنك إضافة مواقع بدون تشفير بمجرد إزالة علامة ✓ على عبارة: "**مطلوب تحقق الملقم** (https:) **لكافة المناطق لهذه المنطقة**".



الشكل رقم (52): تحديد المواقع الموثوقة.

* المواقع غير الموثوقة

هي المواقع التي لا يُوثق بها، ولا بالخدمات التي تقدمها. فقد يُعرف عن تلك المواقع أنها مليئة بالبرامج الخبيثة. ويمكنك إضافة مواقع لهذه القائمة بالطريقة نفسها التي يمكن بها إضافة مواقع لقائمة المواقع الموثوقة، ولكن تحت قائمة المواقع غير الموثوقة.

[4] المستويات الأمنية

قد يتبادر إلى أذهان البعض تساؤل عن الحكمة وراء تحديد المناطق الأمنية، إنها سهولة تحديد مستوى أمني لكل منطقة، وما نعنيه بمستوى أمني هو تحديد الخصائص

الأمنية المسموحة مثل ActiveX وJava. تخيل لو أن هناك منطقة واحدة فقط، وأردت أن تضع لها مستوى أمنياً واحداً لجميع المواقع فهل ستقدر؟ بالتأكيد لن تستطيع، لأنه مع لا يمكن التعامل جميع المواقع بنفس الاحترازات الأمنية. ومتصفح الإنترنت يحتوي على أربعة مستويات أمنية معدة مسبقاً، كما في شكل (53)، لكنها ليست إجبارية، بل يمكنك تكوين الخصائص الأمنية المناسبة حسب رغبتك. لنبدأ بالمستويات الأمنية الأربعة:



الشكل رقم (53): المستويات الأمنية.

عالٍ: هذا المستوى يعزز الجوانب الأمنية إلى الحد الأقصى، ويتفادى - قدر الإمكان- خصائص المتصفح التي قد تؤدي إلى التعدي على النظام. كما هو معروف فإنه كلما زادت المتطلبات الأمنية قلت الخصائص المتاحة. فهذا المستوى، مثلاً، يوقف

عمل ActiveX وJava. ومنطقة المواقع غير الموثوقة تُعطى هذا المستوى مبدئياً.

متوسط: يقدم هذا المستوى قدراً متوسطاً من الحماية، مثل تفادي تنزيل بريمجات ActiveX غير الموقعة إلكترونياً، والتأكد من موافقة المستخدم قبل تنزيل بريمجات ActiveX الموقعة إلكترونياً. يعطى هذا المستوى مبدئياً لمنطقة الإنترنت الخارجية.

متوسط منخفض: مثل مستوى متوسط، لكن بمرونة أكثر، ويعطى هذا المستوى مبدئياً لمنطقة الإنترنت الداخلية.

منخفض: أقل المستويات أماناً، وأكثرها حريةً في استخدام الخصائص المتعددة في المتصفح، ويُعطى مبدئياً لمنطقة المواقع الموثوقة.

[5] إعدادات خاصة

يمكنك العمل بالإعدادات الأمنية المُعدة مسبقاً، أو تغيير بعضها على حسب ما تراه مناسباً لك.لكن ينبغي لك أن تدرك بأن هناك إعدادات كثيرة، وبعضها يحتاج إلى معرفة دقيقة بها، فإذا لم تكن متأكداً من فعلك فلا تغير في الإعدادات الأمنية الدقيقة. ويمكنك الوصول للإعدادات الخاصة كما في شكل (53).

[6] إعدادات الجهاز الافتراضي Virtual Machine (VM)

تتيح هذه الإعدادات للمستخدم تحديد مستوى الأمان للجهاز الافتراضي المتوافق مع بريمجات الجافا، أي يتيح تحديد الإعدادات الأمنية لعمل بريمجات الجافا، و هي مقسمة إلى خمسة مستويات:

مخصص: يتيح للمستخدم التحكم بالصلاحيات يدوياً.

تعطيل جافا: يمنع جميع بريمجات الجافا من العمل.

أمان عال: يسمح لبريمجات الجافا بالعمل فقط في صندوق الرمل.

أمان متوسط: يسمح لبريمجات الجافا بالعمل داخل صندوق الرمل، ويسمح لها بتنفيذ بعض الأعمال خارج الصندوق، مثل: الوصول لمساحة على القرص الصلب خاصة به، وإتاحة الوصول للملفات بتحكم المستخدم.

أمان منخفض: يسمح لبريمجات الجافا بتنفيذ جميع العلميات.

[7] خيارات بريمجات الأكتف إكس

* **تحميل بريمجات الأكتف إكس الموقعة**: لك الخيار في منعها، أو الموافقة، أو طلب رأيك كلما أراد تنزيل بريمجات أكتف إكس موقعة، لكن تعطيلها قد يؤدي إلى حجب خدمات مهمة على صفحات الإنترنت.

* **تحميل بريمجات الأكتف إكس غير الموقعة**: لك الخيار في منعها، أو الموافقة، أو طلب رأيك كلما أراد تنزيل بريمجات أكتف إكس غير موقعة. وفي الغالب البريمجات غير الموقعة مضرة، خاصة إذا أتت من مواقع مشبوهة.

* **تشغيل بريمجات الأكتف إكس**: هذا الخيار يتيح لك التحكم في عمل البريمجات، ويقدم أربع احتمالات: إما أن يكون الخيار بيد مدير النظام، أو بالمنع، أو بالموافقة، أو بطلب رأيك عند كل عمل للبريمجات.

[8] السرية عند استخدام المتصفح

بعض مواقع الإنترنت تستخدم ما يدعى: cookie، أو الكعك، أو ملفات تعريف الارتباط بالمواقع، وهي ملفات نفسية يخزنها الموقع في جهاز المستخدم الذي زار الموقع، لأغراض شتى، منها: معرفة إعدادات المستخدم الشخصية للموقع، لجمع معلومات إحصائية عن زوار الموقع ولأغراض إعلانية. وهناك نوعان من ملفات تعريف الارتباط وهما:

* **ملفات تعريف الارتباط المستديمة**: ولها تاريخ انقضاء يمكن للمتصفح حذفها، وتستخدم لحفظ البيانات لمدة طويلة، مثل اسم الزائر، وبطاقة الائتمان.

* **ملفات تعريف الارتباط الجلسة الواحــدة**: هذه تُستخدم خلال جلسة اتصال واحدة بين الموقع والمستخدم، وتنتهي بإغلاق المتصفح.

وملفات تعريف الارتباط لا تنقل الفيروسات، وليست برامج خبيثة، بل هي ملف نصي يحتوي على بيانات قد تكون مهمة مثل رقم بطاقة الائتمان، أو كلمة مرور، وقد تحتوي على بيانات يمكن من خلالها مراقبة تحركاتك على الإنترنت، والمواقع المزارة. وملفات تعريف الارتباط لا يسمح بقراءتها إلا من كتبها، ويُتحقق من ذلك بالتأكد من النطاق للموقع، ومقارنته بالنطاق الذي في ملفات تعريف الارتباط. ولكن الكعك في الغالب ملفات مهمة لمهاجم النظام لما قد يجده من معلومات مهمة عن المستخدم.

ومتصفح الإنترنت يقدم لوحة تحكم في التعامل مع ملفات تعريف الارتباط، ويحتوي على ستة مستويات (شكل 54)، ويمكنك أيضاً من تحديد شروط أخرى.



الشكل رقم (54): مستويات التعامل مع ملفات تعريف الارتباط.

الخلاصة

المتصفح هو بوابتك إلى الإنترنت، وهي كذلك بوابة غيرك إلى حاسوبك، والمعلومات المخزنة فيه و في بقية الأجهزة المرتبطة بالشبكة التي أنت عضو فيها. ونظراً لشعبية متصفح ميكروسوفت للإنترنت فقد أطلنا النفس في وصف الخطوات اللازمة لتقويته، ونظن أنها تعطي المستخدم قدرا لا بأس به من الحماية.

المساعدات الرقمية الشخصية
Personal Digital Assistant

انتشرت في السنوات الأخيرة المساعدات الرقمية الشخصية (Personal Digital Assistants)، التي يمكن وصفها بأنها هاتف جوال مدمج مع حاسوب صغير جداً، ومن أمثلتها جهاز كيوتك (Qtek)، وآي ميت (I-Mate)، وبلاك بري (Blackberry). ويمكن استخدام هذه الأجهزة لخزن المعلومات، وتشغيل البرامج والاتصالات بالشبكات، تماماً، كما يستخدم الحاسوب العادي .

وقد انتشرت هذه الأجهزة انتشاراً غيى مسبوق، وتفيد التقديرات أن قرابة 50٪ من هذه الأجهزة يستخدم نسخة من نظام التشغيل (Windows)، مما يجعلها عرضة لهجمات القراصنة أصحاب الخبرة في نظام التشغيل هذا[1]. ومن جهة أخرى تشير التقديرات إلى أن أكثر من 80٪ من المساعدات الرقمية يشتريها الأفراد وليس الجهات التي يعملون فيها، مما يجعلها غير خاضعة لسياسات تلك الجهات، خاصة فيما يتعلق بأمن المعلومات[2].

وهناك عاملان يدفعان إلى العناية بالمشكلات الأمنية التي تنجم عن استخدام المساعدات الرقمية، وهذان العاملان هما :

(أ) إمكان ربط المساعدات الرقمية بالشبكة الداخلية لأي منشأة، وفي الوقت نفسه الاتصال لاسلكياً بشبكة الإنترنت، مما يفتح ثغرة في الدفاعات المنصوبة لحماية الشبكة

---

(1) مقال بعنوان: "*Enterprise PDA Policy: Part 2*" للكاتب (J. Gold) نشر في: Meta Group Delta بتاريخ 13 يناير 2002م.

(2) مقال بعنوان: "*PDA TCO: How much?*" للكاتب(J.Gold) نشر في: Meta Group Delta بتاريخ 20 أغسطس 2002م.

الداخلية، كما يعرضها لجميع الأخطار المحدقة بالاتصال اللاسلكي.

(ب) مع تزايد إمكانات المساعدات الرقمية، فإنها أصبحت أداة تنفيذ التطبيقات الكبيرة التي تستخدمها الشركات والمنظمات، وهذه ميزة عظيمة ولا ريب، غير أنها — في الوقت ذاته — تزيد من خطر اختراق تلك التطبيقات من قبل المتطفلين نتيجة لضعف الإجراءات الأمنية الموجودة في المساعدات الرقمية .

ولفهم ما يصاحب استخدام مساعد رقمي معين يجب على المستخدم معرفة أمرين مهمين:

(أ) نظام التشغيل المستخدم في المساعد الرقمي: وأهمية هذا الأمر تأتي من أن الأخطار الأمنية تختلف من نظام تشغيل إلى آخر، فيلزم المستخدم معرفة نظام التشغيل في جهازه ليحدد الاخطار التي قد يتعرض لها جهازه.

(ب) طريقة ربط المساعد الرقمي بالشبكة الداخلية، أو شبكة الإنترنت، ويمكن القول إن هناك طرقاً ثلاثاً للربط هي :

(1) ربط المساعد الرقمي بجهاز حاسوب شخصي باستخدام برامج التناغم (Synchronization Software)، مثل: برنامج (ActiveSync) المستخدم لنظام (Windows)، وبرامج التناغم لا تخلو من الثغرات الأمنية، فبرنامج (ActiveSync)، عندما يعمل يطلب إدخال كلمة عبور (Password)، لكن هذه الكلمة يمكن تخزينها في القرص الصلب للحاسوب الشخصي الذي يرتبط به جهاز المساعد الرقمي. ونتيجة لذلك فإن أي متطفل يخترق النظام الأمني للحاسوب الشخصي يمكنه الوصول إلى المعلومات المخزنة في المساعد أثناء عملية التناغم.

(2) الربط السلكي واللاسلكي باستخدام بطاقة الشبكة (Network Interface Card).

(3) الربط اللاسلكي مثل تقنية البلوتوث والواي فاي:

مما سبق يتضح أن المعلومات المخزنة في المساعد الرقمي عرضة لأخطار أمنية جمة، كما أن ربط المساعد الرقمي بشبكة ما يفتح ثغرة في الحماية المنصوبة حول تلك الشبكة، كما أنه في الوقت ذاته يجعل الجهاز عرضة للهجوم من قبل المهاجمين الذين سبق لهم اختراق الشبكة، وكونوا لأنفسهم موطئ قدم فيها.

[1] الأخطار المصاحبة لاستخدام المساعدات الرقمية الشخصية

إن قائمة الأخطار المصاحبة لاستخدام المساعدات الرقمية الشخصية طويلة جداً. لكن حديثنا سيكون منصباً على أهمها.

(أ) سهولة الحمل

تعد هذه ميزة كبرى للمساعدات الرقمية، غير أنها في الوقت ذاته هي الخطر الأكبر المحدق بها. فسهولة حمل الجهاز يجعله عرضه للسرقة أو الضياع أكثر من غيره، وبذلك يمكن استخدامه لتخطي الحواجز الأمنية المنصوبة حول الشبكة التي يسمح للجهاز بالاتصال بها. ولمعرفة حجم هذه المشكلة علينا أن نستحضر بعض الدراسات التي تفيد بأن ما يقارب 250.000 جهاز مساعد رقمي فقدت في المطارات الأمريكية في عام 2001م(1)، ولاشك أن الرقم ازداد تبعاً لزيادة اقتناء الناس للمساعدات الرقمية.

(ب) ضعف وسائل الحماية الأصلية التي تأتي مع المساعدات

(1) مقال بعنوان: "*What Does Trustworthy Computing Mean for Pocket PC?*" للكتاب: (D. Wiggins, R. Simpson, D. McHugh)، و نشرتها Gartner Inc. Research Note في 27 أغسطس 2002م.

الرقمية من الشركات المصنعة، مثل:

(1) ضعف تشفير كلمات العبور (Password).

(2) إمكان تجاوز آلية كلمات العبور بتغيير إعدادات الجهاز.

(جـ) البرامــج الخبيثة (Malicious Software):

من مميزات المساعدات الرقمية حيازتها معالجاً وتخزيناً يكفيان لحفظ ملفات المعلومات، وتشغيل البرامج، وهذه الميزة تجعلها أيضاً هدفاً للبرامج الخبيثة، كالفيروسات والديدان التي تنتقل من المساعد الرقمي إلى الحاسوب العادي والعكس عند ربط هذين الجهازين. وعندما يكون الحاسوب العادي جزءاً من شبكة بها معلومات مهمة، فإن ربط مساعد رقمي بالحاسوب لغرض التناغم، أو نقل الملفات يفتح ثغرة، يمكن أن تتسلل منها البرامج السيئة إلى الشبكة، انطلاقاً من المساعد الرقمي، ومروراً بالحاسوب العادي.

ومن أمثلة الفيروسات التي تهاجم المساعدات الرقمية المعتمدة على نظام التشغيل (Windows CE) فيروس (WinCE4.Dust)، وهذا الفيروس يمكنه مهاجمة الملفات من نوع (exe) المخزنة في المساعد الرقمي، ولكن الهدف من تطويره كان مجرد لفت الانتباه إلى أن مثل هذا الفيروس يمكن تطويره، وقد ظهر قريباً واحد من أحصنة طروادة يسمى (Backdoor.Brador.A)، وهذا البرنامج السيئ إذا حملته في مساعدك الرقمي، فإنه يفتح قناة اتصال مع جهاز الشخص الذي طوره، ويُمكِّن ذلك الشخص من مساعدك الرقمي، فيصبح قادراً على تحميل الملفات والبرامج إلى مساعدك الرقمي، وتنفيذها، وحذفها، واستعراض الملفات الموجودة في مساعدك الرقمي، وهلم جرا[1].

(د) الهندسة الاجتماعية

(1) مقال على الرابط : [http://www.cewindons.net/faqs.net/faqs/ppc-ar.htm]

هناك صلة وثيقة بين الخطر الناجم عن سرقة المساعد الرقمي الشخصي أو فقدانه والهندسة الاجتماعية ، وذلك أن المعلومات الموجودة في المساعد الرقمي المسروق تتيح أمام المهاجم باستخدام الهندسة الاجتماعية كما ضخما من المعلومات التي يمكنه استخدامها للحصول على مزيد من المعلومات.

(هـ) الاتصال اللاسلكي بين المساعد الرقمي والأجهزة المناظرة أو الشبكات

كان هذا الاتصال - ومازال- البوابة التي يسهل ولوج المهاجم منها ، نتيجة لطبيعة الاتصال اللاسلكي ، والثغرات الموجودة في الإجراءات الأمنية المتبعة في تقنيات الاتصال اللاسلكي ، كالبلوتوث والواي فاي.

[2] كيفية التقليل من الاخطار المصاحبة لاستخدام المساعدات الرقمية الشخصية

سنتطرق في هذا الجزء من الكتاب لعدد من السبل الممكن اتخاذها لتقليل تلك الأخطار ، ومن هذه السبل ما هو على مستوى المنشآت ، ومنها ما هو على مستوى الأفراد.

وضع سياسات تضبط استخدام المساعدات الرقمية الشخصية في المؤسسات والشركات ونحوها ، ويجب أن تنظم هذه السياسات الأمور التالية :

(1) تحديد الاستخدام الأمثل للمساعدات الرقمية في محيط العمل داخل المنشأة.

(2) تحديد طريقة اقتناء المساعدات الرقمية داخل المنشأة.

(3) تحديد الإعدادات التشغيلية والأمنية التي يجب أن يجهز بموجبها كل مساعد رقمي.

(4) تقديم الدعم الفني لمستخدمي المساعدات الرقمية ، مما يسهل لأخصائي تقنية المعلومات متابعة كيفية استخدام هذه الأجهزة ، والتنبيه عن أي خطر قد يتسلل إلى البنية المعلوماتية للمنشأة من قبل هذه الأجهزة.

(5) تنميط (Standardization) البرامج والأجهزة التي تستخدم مع المساعدات الرقمية. فإذا اعتمدت منشأه برنامج تناغم معيناً، فإن تحديد الثغرات الأمنية الموجودة في ذلك البرنامج أمر سهل، وبالتالي يكون التعامل الصحيح مع الثغرات الموجودة فيه أمرا ممكنا. أما إذا ترك الحبل على الغارب لمستخدمي المساعدات الرقمية فسيكون على المسؤولين عن أمن المعلومات في المنشأة التعامل مع عدد كبير من برامج التناغم، وبالتالي عليهم التعرف على عدد كبير من الثغرات، مما يصعب اتخاذ خطوات احترازية ضدها.

(6) استخدام وسائل توثيق الهوية (Authentication Tools) التي توفر قدراً ملائما من الحماية بدلاً من الاعتماد على ما هو موجود أصلاً في المساعدات الرقمية. ومما يجب أن تتحلى به وسائل توثيق الهوية الجيدة ما يلي:

(أ) استخدام الأسلوب المركزي في إدارة كلمات المرور للتحقق من موافقتها للسياسات المعتمدة لأمن كلمات المرور، مثل: قوة الكلمات المستخدمة، وأنها تغير بشكل دوري.

(ب) وجود إجراءات مضادة لطرائق الهجوم الشائعة التي تهدف إلى تقويض كلمة المرور.

(جـ) برمجة المساعد الرقمي بحيث يقوم بحذف الملفات المخزنة فيه تلقائيا عند اكتشاف محاولات اختراق آليات الحماية الموجودة فيه.

(د) وجود الآليات المناسبة لتشفير كلمات المرور.

(هـ) استخدام أدوات التعريف المعتمدة على الخصائص البيولوجية للمستخدم (Biometrics) للتحقق من الهوية، مثل البصمة، والتعرف على التوقيع، والتعرف على الصوت.

(7) استخدام تقنيات التشفير لحماية المعلومات المخزّنة في المساعد الرقمي، وحماية الاتصال بين المساعد الرقمي والحاسوب العادي.

(8) تحميل برامج الحماية مثل البرامج المضادة للفيروسات والديدان وغيرها من البرامج السيئة. ومن أمثلة برامج الحماية برنامج (Airscacanner Mobile).

(9) الاستفادة من الحلول المتكاملة للحماية (Integrated Security Tools) التي بدأت تظهر أخيراً، ومن مزاياها محاولتها التعامل في آن واحد مع عدد كبير من المشكلات الأفقية للمساعدات الرقمية.

(10) تحميل برنامج جدار حماية في المساعد الرقمي لكبح أي محاولة غير مشروعة لإنشاء اتصال مع الجهاز.

(11) وضع برامج التناغم على وضع الإطفاء (Off) عندما لا تكون مستخدمة.

(12) تجنب تخزين كلمة المرور الخاصة بعملية التناغم على الحاسوب العادي.

(13) التحقق من متابعة التحديثات الأمنية وتنزيلها بشكل موقوت إلى المساعدات الرقمية.

(14) تجنب استخدام المساعدات الرقمية التي فيها معلومات حساسة في الأماكن العامة.

الخلاصة

المساعدات الرقمية – بلا شك– ذات فوائد عظيمة، لكنها مثل باقي معطيات التقنية الحديثة سلاح ذو حدين. و للاستفادة القصوى منها على الإنسان التعرف على المحاذير المحيطة باستخدامها لتجنبها. أما على مستوى المنشآت فإن حماية أنظمة المعلومات من الأخطار التي تجلبها المساعدات الرقمية يتطلب عددا من الإجراءات التي قد يترتب عليها إدخال تغييرات في بيئة العمل.

البلوتوث

Bluetooth

كسبت تقنية البلوتوث (Bluetooth) زخماً جديداً، ويتوقع أن يصل عدد الأجهزة المزودة بها إلى 971 مليون جهاز بحلول عام 2006م. وعلى الرغم من اكتساحها الأسواق بسبب ما توفره من خدمة فإن التصميم الداخلي لهذه التقنية به ثغرات كبيرة ومتعددة، مما يُسهل للمهاجم شن هجمات من قبيل التصنت، وانتحال الشخصية، وسرقة المعلومات، والحرمان من الخدمة. وقبل الخوض في الأخطار التي تحف استخدام تقنية البلوتوث، والاحترازات التي يمكن اتخاذها لتخفيف تلك الأخطار، سنتحدث عن التقنية نفسها بشكل مبسط، والخصائص الأمنية الداخلية فيها.

[1] ما هو البلوتوث؟

هو مجموعة من المواصفات توضح طريقة لربط الأجهزة الإلكترونية لاسلكياً، وهذا الربط إنما يكون لمسافات قصيرة، والتقنية الحالية تسمح بربط فعال للأجهزة التي تصل المسافات بينها إلى حدود عشرة أمتار، ويمكن استخدام تقنية البلوتوث لربط أنواع مختلفة من الأجهزة بعضها ببعض، ومن أمثلة ذلك:

* ربط هاتف جوال بسماعة الأذن.
* ربط هاتف جوال بحاسوب محمول.
* ربط جهاز حاسوب محمول بحاسوب عادي.
* ربط لوحة المفاتيح بالحاسوب.
* ربط الفأرة بالحاسوب.
* ربط جوال بجوال آخر.

[2] كيف يعمل البلوتوث؟

صمم البولتوث ليعمل على النطاق المسمى(Industrial Scientific Medicine)، والذي يعرف باختصار باسم (ISM)، وتردده يتراوح داخل النطاق (GHZ 2.4835-2.4) في معظم دول العالم.

ويمكن ربط جهازين أو أكثر لتكوين ما يسمى (Piconet)، ويجب أن يقوم أحد الأجهزة المشاركة في (Piconet) بدور المتبوع(Master) ، بينما تقوم كل من الأجهزة الأخرى بدور التابع (Slave)، ويمكن ربط سبعة أجهزة كحد أقصى في (Piconet) واحدة.

[3] الخصائص الأمنية في البلوتوث

لم يأت البلوتوث خلواً من أي خصيصة أمنية، ولكن خصائصه الأمنية على مستوى الربط (Link) وليس التطبيقات (Applications)، وهذا يتيح قدراً من المرونة لمصممي التطبيقات التي تستخدم تقنية البلوتوث بمعنى أن يصبح المصمم حرا في استخدام التقنية التي يراها مناسبة. ومن الخدمات الأمنية التي جاءت مع تقنية البلوتوث ما يلي:

(أ) خدمة سرية المعلومات.

(ب) خدمة التحقق من هوية الجهاز المتصل.

(جـ) خدمة التحقق من أن الجهاز المتصل مخول بالاطلاع على المعلومات المخزنة في الجهاز المتصل به.

يضاف إلى ما سبق أن خصائص البلوتوث تتيح تقسيم النطاق الترددي (ISM) إلى 79 قناة، ما يؤدي إلى إمكانية قفز الأجهزة المتصل بعضها ببعض من قناة إلى أخرى بصورة جماعية. وهذا من شأنه التخفيف من تداخل الإرسال اللاسلكي بين الأجهزة التي تستخدم البلوتوث، وأي أجهزة إلكترونية أخرى تعمل في النطاق الترددي (ISM).

كما أن أسلوب القفز بين القنوات المختلفة يصعب التصنت على المعلومات المتبادلة بين الأجهزة التي يتصل بعضها ببعض مستخدمة تقنية البلوتوث.

[4] نقاط الضعف في البلوتوث

يسبق تبادل المعلومات بين جهازين فيهما تقنية البلوتوث تأسيس الارتباط، وهو ما يعرف بعملية (Pairing)، وفي هذه العملية يتبادل الجهازان بيانات معينة لبناء نوع من الثقة بينهما. ولحماية المعلومات التي ستتبادل في عملية الاتصال الحقيقي بعد الانتهاء من مرحلة تأسيس الارتباط. ومرحلة تأسيس الارتباط هي أخطر المراحل؛ لأن البيانات التي تتبادل فيها غير مشفرة، مما يجعلها عرضة للالتقاط من المتطفلين، الذين يمكنهم استخدامها في شق أنواع متعددة من الهجمات.

ومن نقاط الضعف أن الجهاز المزود بتقنية البلوتوث يمكن أن يعمل في أي من عدة أوضاع، بعضها يجعل البيانات المخزنة في الجهاز عرضة للخطر، وهذه الأوضاع هي:

(أ) وضع "قابل للاكتشاف"، ووضع "غير قابل للاكتشاف"، أو(Discoverable) و(non–Discoverable): وفي الوضع الأول يستجيب الجهاز لأي استفسار (Inquiry) يأتيه من جهاز آخر.

(ب) وضع " قابل للارتباط "، ووضع " غير قابل للارتباط"، وفي الوضع الأول يستجيب الجهاز لأي رسالة تأتيه من جهاز آخر سبق اكتشافه.

[5] طرق الهجوم على البلوتوث

سنتحدث في هذا الجزء عن عدد من الطرق التي يمكن استخدامها في شن الهجمات على الأجهزة المزودة بتقنية البلوتوث.

(أ) استغلال الثغرات الموجودة بسبب أوضاع التهيئة الأصلية (**Default Configuration**) للجهاز

ويقصد بها الأوضاع أو الإعدادات الأولية التي يكون عليها الجهاز عند خروجه من المصنع وعرضه للبيع. وأكثر الأجهزة اليوم توفر خدمات كثيرة، مما يصعب على المستخدم العادي تحديد الأوضاع الصحيحة، ولذا تلجأ الشركات المصنعة إلى إخراج منتجاتها إلى السوق، وقد أعدت تلك الأجهزة بأوضاع معينة، أو ما يسميه بعضهم الإعدادات الأصلية للجهاز.

ومن الإعدادات الأصلية التي يعملها بعض مصنعي الأجهزة: جعل خاصية الإرسال والاستقبال على وضع التشغيل (On). وعندما يكون الجهاز في هذا الوضع فإنه يتبادل بعض المعلومات تلقائياً مع أي جهاز مزود بتقنية البلوتوث، بمجرد أن يصبح الجهازان على مقربة بعضهما من بعض. ومن المعلومات التي يتبادلانها العنوان الرقمي المعرف للجهاز، والوقت، وهاتان المعلومتان تستخدمان في حسابات مفاتيح التشفير عندما يريد جهازان الاتصال بعضهما ببعض. والجدير ذكره أن هذا التبادل الذي كان بسبب الإعدادات الأولية للجهاز يجري دون علم صاحب الجهاز، والخطورة هنا أن بإمكان شخص ما لديه جهاز مزود بالبلوتوث أن يذهب بالقرب من شخص آخر يعرف أن لديه جهازاً مزوداً بالبلوتوث، وإعداداته الأولية كما جاءت من المصنع، وينشئ معه اتصالاً يحصل منه على المعلومتين السابقتين اللتين يمكن استغلالهما فيما يلي:

(1) انتحال شخصية صاحب الجهاز الذي مازالت إعداداته الأولية كما جاءت من المصنع.

(2) التصنت على أي تبادل معلومات باستخدام البلوتوث يجريه صاحب الجهاز الذي لم تغير إعداداته.

(3) متابعة صاحب الجهاز ومراقبة الأماكن التي يرتادها لأغراض التجسس عليه، وجمع المعلومات عنه.

وغالباً ما يقوم المصنع باختيار الإعدادات الأصلية التي توفر أقل قدر من الحماية، أو التي لا توفر أي حماية على الإطلاق؛ لأن ذلك يسهل على المستخدم الاستفادة من وظائف الجهاز بشكل أكبر مما لو هيأت الإعدادات الأصلية بحيث تشغل إجراءات الحماية.

(ب) السرقة أو ضياع الجهاز

مع توالي التقدم التقني تصبح الأجهزة أصغر حجماً وأخف وزناً، وهذا يسهل نقلها، لكن سهولة نقلها يجعلها أكثر عرضة للسرقة أو الضياع. وتشير إحدى الدراسات إلى أن منظمة الضرائب الأمريكية (IRS) فقدت 2332 جهازا من أجهزة الحاسوب المحمول خلال ثلاث سنوات فقط، والخطر الذي تمثله سرقة الأجهزة أو فقدانها مصدره بالطبع المعلومات المخزنة فيها. فالجهاز المفقود - إذا كان مزودا بتقنية البلوتوث ولم تغير إعداداته الأصلية - يحتفظ بمفاتيح التشفير التي يستخدمها للاتصال بالأجهزة التي سبق له فيما مضى تأسيس ارتباط معها، وبالتالي فإن ضياع جهاز واحد أو سرقته قد يعرض كل الأجهزة الأخرى التي سبق لها تأسيس ارتباط معه إلى أخطار منها:

(1) يمكن استخدام الجهاز المسروق أو المفقود للتنصت على الاتصالات التي تجري بين الأجهزة التي سبق له الارتباط بها.

(2) إنشاء اتصال مع أي من هذه الأجهزة باستخدام الجهاز المسروق، ونقل المعلومات منها.

(3) استخدام الجهاز المسروق لإنشاء اتصال مع حاسوب ذي معالج أكثر قوة من الجهاز المسروق، ثم استغلال ذلك الجهاز القوي لشن هجمات أكثر تعقيداً مما يتيحه الجهاز المسروق.

(4) جمع معلومات عن الشخص صاحب الجهاز المسروق وعلاقاته

بالأشخاص الذين لديهم أجهزة سبق له الارتباط بها.

(جـ) التنصت (Eavesdropping)

لإحباط هذا النوع من الهجوم زودت تقنية البلوتوث بخصيصة القفز بين الترددات المختلفة. وعند إنشاء الاتصال تجري الأجهزة التي تريد الاتصال بعضها ببعض عدة عمليات حسابية لتحديد عدد من القنوات ضمن النطاق الترددي بحيث تقفز الأجهزة بين هذه الترددات، وتستخدم في هذه العمليات الحسابية الرقم المعرف للجهاز المتبوع والوقت المسجل، كما أن عملية القفز بين الترددات تجري بسرعة (1600) مرة في الثانية الواحدة.

لكن أسلوب القفز بين الترددات يمكن التغلب عليه باستخدام أجهزة تتنصت على النطاق الترددي كله في آن واحد.كما أن هناك طريقة أخرى للتغلب على القفز بين الترددات، كون الجهاز المتبوع يستجيب لأي استفسار يأتيه عن رقمه المعرِف والوقت عنده، وهذا كل ما يحتاجه المهاجم لتحديد الترددات التي يقفز بينها الجهاز المستهدف، وبالتالي يستطيع المهاجم القفز مع المستهدف والتنصت على الاتصال.

من جهة أخرى فإن تقنية البلوتوث تستخدم نوعاً من التشفير للحد من التنصت على تبادل المعلومات بين الأجهزة المتصلة. لكن يُضعف هذا التشفير أن المعلومات التي تستخدم مادة لصنع مفاتيح التشفير تُرسَل عند تأسيس الارتباط غير مشفرة، فيمكن التقاطها ومعرفة المفاتيح التي ستستخدم في التشفير، مما يجعل التشفير غير ذي فائدة.

ولو افترضنا أن شخصاً ما فقد سماعة الهاتف الجوال المزود بتقنية البلوتوث فإن من يجد هذه السماعة يمكنه التنصت على اتصالات صاحب الهاتف الجوال؛ وذلك لأنه قد سبق تأسيس ارتباط بين الجوال والسماعة، مما جعل من السماعة أداة المعلومات اللازمة لإنشاء الاتصال مع الجوال في أي وقت. كما أن هذه المعلومات تمكن السماعة من فك التشفير الذي يستخدمه الجوال أثناء الاتصال. كما يمكن استغلال السماعة بجعلها تنتحل

شخصية الهاتف الجوال لتتصل بالحاسوب المحمول لتحقيق مزيد من الاختراق، وجمع مزيد من المعلومات عن الشخص المستهدف.

[6] وسائل الحماية من الهجوم على تقنية البلوتوث

يجب أن يُعلم أن الوسائل التي نعرضها هنا لا توفر حماية تامة، بيد أنها تقلل من الأخطار الناجمة عن طرق الهجوم التي أشرنا إلى بعضها فيما سبق. ومن أهم الوسائل ما يأتي:

(أ) ضبط تهيئة الجهاز بما يوفر القدر الملائم من الحماية.

(ب) اختيار رقم سري طويل، حتى تصبح محاولة معرفته أكثر صعوبة .

(جـ) ضبط الجهاز على وضع "غير قابل للاكتشاف" طوال الوقت، وعند الحاجة إلى تأسيس ارتباط يمكن تحويله إلى وضع "قابل للاكتشاف"، ثم يعاد إلى وضع "غير قابل للاكتشاف" بعد ذلك .

(د) تجنب إجراء عملية تأسيس الارتباط في مكان عام .

(هـ) تشغيل إجراءات الحماية التي مع بعض التطبيقات تعتمد على تقنية البلوتوث.

الخلاصة

تقنية البلوتوث تسهم في زيادة رفاهية المستخدمين، ويُتوقع ألا يخلو جهاز إلكتروني منها في المستقبل القريب جدا. و نظرا لوجود عدد من الثغرات الأمنية فيها، و لكونها غالبا ما تستخدم بصفة شخصية فإننا ننبه القارئ الكريم إلى ضرورة الإلمام بأساليب الهجوم، وتقنيات الدفاع، خاصة ما يتعلق بضبط تهيئة الجهاز، واختيار الرقم السري.

الحواسيب المحمولة
Laptop

أصبحت الحواسيب المحمولة (Laptops) من ضروريات الحياة لكثير من الناس ؛ لما تقدمه من خدمات، وتمتاز به من مزايا أهمها : صغر الحجم، وخفة الوزن. وكما هو الحال في الأجهزة الأخرى فإن تلك المزايا نفسها هي ما تجعل الحواسيب المحمولة عرضة للأخطار.

[1] الأخطار التي تحدق بالحواسيب المحمولة

(أ) السرقة

يسيل لعاب اللصوص عند رؤية جهاز محمول، وهؤلاء لا يكترثون كثيرا بالمعلومات المخزنة في الجهاز ؛ إذ لا هم لهم سوى الاستفادة من الجهاز نفسه، سواء باستخدامه، أو بيعه والاستفادة من ثمنه.

(ب) التجسس

يسعى الجواسيس أو سارقو المعلومات إلى الوصول إلى المعلومات المخزنة في الأجهزة المحمولة، وهنا لا يمثل الجهاز نفسه هدفاً، وإنما المستهدف هو المعلومة المخزنة فيه. و من التجسس ما يكون لكشف معلومات ذات أهمية سياسية كما يحدث بين الدول، أو للحصول على معلومات ذات أهمية تقنية كالتجسس الصناعي.

(جـ) الضياع

وينتج عن هذا - بطبيعة الحال - فقدان جميع المعومات المخزنة فيه ما لم تكن هناك نسخ احتياطية منها.

(د) التلف

بسبب خفة وزن هذه الأجهزة ؛ وسهوبه حملها تكون معرضة للسقوط من يد

حاملها، كما أنها قد توضع في أماكن تعرضها للحرارة العالية أو البرودة الشديدة.

و لاشك أن سرقة جهاز لبيعه أو استخدامه مشكلة للجهة التي فقدت الجهاز، كونها قد تكبدت خسارة تتمثل في ثمن الجهاز المسروق، ولكن المشكلة الحقيقية هي في قيمة المعلومات الموجودة فيه، خاصة إذا لم تكن هناك نسخة احتياطية لتلك المعلومات، فقد تكون الجهة المالكة لتلك المعلومات قد أنفقت كثيراً من الوقت والمال من أجل الوصول إلى تلك المعلومات أو جمعها. وإذا كانت المعلومات متعلقة بأمور حساسة يؤثر كشفها في قدرة الشركة التنافسية مثل: المصاعب التي تواجهها الشركة، أو المعلومات السرية المتعلقة بمنتجات الشركة، فإن هذا -ولا شك- يمثل كبوة قد لا تستطيع الشركة النهوض منها. وأسوأ من هذا أو مثله ما إذا كان الجهاز المسروق يحوي معلومات حساسة لأفراد من عملاء الشركة، فمثل هذه المعلومات يجب على الشركة حمايتها، وفي حال كشفها تصبح الشركة عرضة للملاحقات القانونية من قبل الأفراد، وغالبا ما يترتب على هذا إلزام الشركة بدفع تعويضات باهظة قد تطيح بالشركة.

وقد صرح بعض السارقين أن المال والحواسيب المحمولة والمجوهرات هي الأشياء المفضلة لديهم[1]. وتدل الوقائع والإحصاءات أن للأجهزة المحمولة جاذبية شديدة تجعل بعض المتربصين يقتحم الأخطار من أجل وضع أيديهم عليها. و فيما يلي بعض الأمثلة على هذا:

(أ) بعد أن فرغ المدير التنفيذي لشركة (Qualcomm) – إحدى شركات الاتصالات في الولايات المتحدة – من تقديم محاضرة في قاعة محاضرات أحد الفنادق تقدم للحديث مع الصحفيين، ومراسلي القنوات التلفزيونية الذين كانوا يغطون المحاضرة، وترك حاسوبه

(1) هيئة الإذاعة والتلفزيون البريطانية في 7 نوفمبر 2004م.

المحمول على منصة الإلقاء التي لم تكن تبعد عنه أكثر من عشرة أمتار. و لما فرغ من حديثه التفت إلى منصة الإلقاء ليجد أن حاسوبه المحمول قد سرق(1).

(ب) سرق حاسوب محمول يستخدمه أحد موظفي بنك أمريكا (Bank of America) من سيارة الموظف، ويخزن هذا الحاسوب أسماء وعناوين وأرقام هوية 18 ألف شخص من عملاء البنك(2).

(جـ) يسرق واحد من كل 8 حواسيب محمولة حسب إحصاءات مكتب التحقيقات الفدرالي الأمريكي(3).

(د) يسرق في أمريكا 1600 حاسوب محمول يوميا(4).

ويكون الحاسوب أكثر عرضة للأخطار المذكورة آنفا، خاصة السرقة عندما يشعر مستخدمه بالاطمئنان، ولا يتخذ أي إجراءات احترازية لحماية الجهاز، وقديما قيل "يؤتى الحذر من مأمنه".

[2] حماية الحواسيب المحمولة

تتطلب حماية الحواسيب المحمولة - كغيرها من أوعية حفظ المعلومات- مزيجا من الإجراءات الإدارية، والوسائل الفنية، ووسائل الحماية الحسية Physical Security، ولا غنى لإحداها عن الأخرى، وعلى القارئ الكريم مراعاة أن منها ما هو صالح للتطبيق من قبل الأفراد، ومنها ما هو خاص بالجهات، شركات كانت، أم دوائر حكومية.

---

(1) مقال بعنوان: Data Confidentiality in an Electronic Environment في الموقع:
http://www.nysscpa.org/cpajournal/2003/0303/features/f032403.htm

(2) San Francisco Chronicle, June 28, 2005.

(3) مقال بعنوان: Security News Highlights في الموقع:
http://www.inspice.com/aprod-code/doc/ITR-laptop-theft-news.htm

(4) Time Magazine, January 27, 2003.

(أ) الإجراءات الإدارية

هناك عدد من هذه الإجراءات، ولكننا سنقصر الحديث على أهمها:

(1) وضع سياسة شاملة لأمن المعلومات، والموارد الحاسوبية بحيث يكون من مكونات هذه السياسة تصنيف للمعلومات بحسب حساسيتها للجهة المعنية، وتحديد ما يمكن تحميله منها من الشبكة الخاصة بالجهة إلى الحاسوب المحمول.

(2) وضع تنظيم يحدد الأماكن التي يسمح للموظفين بأخذ الأجهزة المحمولة إليها أو تركها فيها.

(3) تنظيم عملية الدخول، وتأمين الحماية المستمرة للأماكن التي توجد فيها الأجهزة المحمولة؛ لأن الإحصاءات تدل على أن 40٪ من سرقة الأجهزة المحمولة إنما يقع في مكاتب الجهات المالكة للأجهزة[1].

(4) وضع إجراءات لحماية الحواسيب المحمولة عند السفر جواً أو براً، وعند حضور المؤتمرات والندوات، وتدريب الموظفين على ذلك. ومن هذه الإجراءات، مثلاً، تجنب ترك الأجهزة في الحجرة الخلفية للسيارة، لأن ذلك يعرضها للعوامل الجوية، مثل: الحرارة المرتفعة التي قد تتلف الدوائر الإلكترونية في الحاسوب، أو البرودة الشديدة التي تؤدي إلى عطب شاشة الحاسوب. كما أن ترك الحاسوب في الحجرة الخلفية أو داخل مقصورة القيادة قد يؤدي إلى سرقة الجهاز، وهناك عصابات وأفراد متخصصون في سرقة الأجهزة المحمولة خاصة من السيارات المستأجرة. كما يجب توجيه اهتمام خاص بإجراءات أمن الأجهزة المحمولة عند حضور المؤتمرات والندوات؛ وذلك لأسباب منها: أن هذه المحافل تتميز غالبا بضعف الإجراءات الأمنية، ويصاحب ذلك شعور وهمي بالأمن، نظراً لأن غالب من يحضر هذه المحافل من المتخصصين في

---

(1) مقال بعنوان: Laptop Security Guidelines في الموقع:
http://labmice.techtarget.com/articles/laptopsecurity.htm

موضوع المؤتمر أو الندوة، والحقيقة أن هناك أشخاصاً متخصصين في سرقة هذه الأجهزة من قاعات المؤتمرات والندوات، وهؤلاء يسهل عليهم التسلل إلى القاعات، خاصة إذا كانت النشاطات تمتد عدة أيام؛ وذلك لأن التحقق من الهويات يكون غالبا في اليوم الأول، كما أن طول فترة المؤتمر يكون مدعاة لاسترخاء الحس الأمني في أوساط الحاضرين.

(5) وضع ملصقات على الجهاز المحمول تبين اسم الجهة المالكة للجهاز، ويجب أن يكون من الصعب نزع هذه الملصقات. وهذا الإجراء قد لا يمنع سرقة الجهاز، ولكنه قد يعين في استرداده، خاصة إذا اكتشفت السرقة بسرعة. وبحسب إحصاءات مكتب التحقيقات الفدرالي الأمريكي فإن 97٪ من الأجهزة المسروقة التي ليس عليها أي ملصقات تعريفية لا يعثر عليها[1].

(6) عمل نسخ احتياطية للمعلومات المخزنة في الجهاز المحمول يمكن الرجوع إليها في حال سرق الجهاز، ويجب أن تعمل هذه النسخ بشكل دوري بحيث تكون النسخ الاحتياطية متفقة إلى أقصى حد مع ما هو مخزن في الجهاز. كما يجب أن يقوم مالك الجهاز – شخصا كان أو جهة – بالتحقق من أنه بالإمكان استعادة النسخ الاحتياطية وتحميلها إلى جهاز آخر في حال فقدان الجهاز الأصلي أو تلفه. وقد سبق الحديث عن عمل النسخ الاحتياطية في فصل آخر.

(7) تسجيل الجهاز عند الشركة المصنعة أو الموردة؛ لأن ذلك مما يساعد في استرجاعه إذا سرق؛ وذلك لأن السارق قد يحتاج يوما إلى إرسال الجهاز للإصلاح أو الصيانة، وإذا تحققت الشركة من رقم الجهاز فإنها ستكتشف أن الجهاز مسروق، مما يعين في إرجاعه إلى مالكه الأصلي.

---

(1) المرجع السابق.

(ب) الوسائل الفنية

هناك عدد من الوسائل التي يمكن اتخاذها لحماية الحواسيب المحمولة ؛ ولكننا سنقصر الحديث على أهمها :

(1) استخدام كلمة مرور قوية لتصعيب مهمة من يريد الحصول على المعلومات المخزنة في الجهاز في حال سرق الجهاز. و قد ناقشنا في فصل سابق كيف يمكننا جعل كلمات المرور قوية.

(2) استخدام إجراءات الحماية القوية مثل البطاقات الذكية (Smart Cards) ، وأدوات التعريف المعتمدة على الخصائص البيولوجية للمستخدم وهو ما يعرف بالـ (Biometrics) مثل البصمة. و قد ناقشنا في فصل سابق هذه الإجراءات.

(3) وضع كلمة مرور قوية للنظام الأساس (BIOS) لحرمان مستهدفي المعلومات المخزنة في الجهاز من الوصول إليها بسهولة.

(4) تحميل برنامج خفي يسهل متابعة الجهاز المحمول بحيث يقوم هذا البرنامج بالاتصال ببرنامج آخر كلما ارتبط المحمول بشبكة الإنترنت. ويمكن أن يكون البرنامج المتصل به مخزنا في الجهاز الخادم الخاص بالشركة المالكة للجهاز المحمول. وفائدة هذا البرنامج تتضح في حال سرقة الجهاز. فعندما يحاول السارق استخدام الجهاز للاتصال بشبكة الإنترنت يجري البرنامج الموجود في المحمول اتصالا بالبرنامج الموجود في الخادم، ويمرر معلومات عن موقع الجهاز المسروق -عنوانه الرقمي - ، وأي معلومات أخرى قد تؤدي إلى استرجاع الجهاز المسروق. وهذا الحل يستلزم تعاون جهات عدة ، منها شركة الاتصالات ، والشرطة ، والشركة المزودة لخدمة الإنترنت لتحديد موقع الجهاز المسروق.

(5) تشفير المعلومات المخزنة في الجهاز ، وهذا قد يكون مفيدا ضد من غايتهم التجسس.

(6) استخدام جدران الحماية الشخصية لحماية المعلومات المخزنة في الجهاز من المتلصصين، ومن البرامج السيئة. ومع أن هذا الإجراء يوصى به لكل أجهزة الحاسوب، فإنه يكون مؤكداً عند استخدام الحواسيب المحمولة؛ وذلك لأن الحواسيب العادية غالبا ما تستخدم في مقر الشركة وضمن شبكتها، وكثير من الشركات تضع جدرانا نارية لوقاية شبكتها والحواسيب، المرتبطة بالشبكة من الشرور القادمة من الإنترنت. ولكن الجهاز المحمول قد يخرج به المستخدم إلى خارج مقر الشركة، ويربطه بشبكة الإنترنت مباشرة، وهنا يصبح الجهاز المحمول عرضة لهجمات المتلصصين، والبرامج السيئة. وقد سبق الحديث عن جدران الحماية في فصل سابق من الكتاب.

(7) تطبيق الإجراءات الفنية المناسبة للتخلص من البيانات المخزنة في الأجهزة المحمولة، وذلك عند الرغبة في بيع الجهاز المحمول أو إعطائه إلى موظف آخر، و قد سبق الحديث عن طمس البيانات في فصل مضى.

(جـ) وسائل الحماية الحسية

تعج محلات معدات الحاسوب بالمعدات المتخصصة لتأمين الحماية الحسية للحواسيب المحمولة، ومن أهم ذلك ما يلي:

(1) سلك الأمان الذي يربط في موضع خاص يسمى: (Universal Security Slot) بالحاسوب المحمول، و أكثر من 80٪ من الحواسيب المحمولة مزود بهذه الميزة[1]. ويكمن تثبيت الكيبل بهذا الموضع كما في الشكل (55)، كما يثبت طرفه الآخر بجسم ثقيل جدا أو ثابت[2]. ومثل هذا الإجراء لا يمنع اللص المترصد المزود بالمعدات

---

(1) مقال بعنوان: Laptop Security Guidelines في موقع:
http://labmice.techtarget.com/articles/laptopsecurity.htm

(2) من الموقع: http://www.computersecurity.com/laptop/cables.htm

المناسبة، لكنه يصعب مهمة اللص العادي.



الشكل رقم (55): سلك الأمان.

(2) سبق أن أشرنا إلى أن 40٪ من حالات سرقة الحواسيب المحمولة تقع في مقر الشركة المالكة للجهاز، والسراق بالتالي هم من العاملين في الشركة، أو عامل النظافة فيها، أو من المتعاقدين الذين يصرح لهم بدخول مقر الشركة. وللحد من هذا تستخدم محطة تثبيت (Docking Station) بحيث يوضع الجهاز عليها. ويجب أن تكون المحطة محكمة التثبيت بالمكتب التي هي عليه، كما يجب أن تكون فيها خاصية تثبيت وربط الجهاز المحمول بها بحيث لا يمكن فصله عنها إلا بالمفتاح المناسب.

(3) تجنب استخدام الحقائب المخصصة لحمل الحواسيب المحمولة، لأنها بمثابة توجيه دعوة لسرقة الحاسوب المحمول.

الخلاصة

لم يعد استخدام الحواسيب المحمولة وقفا على فئة بعينها. و قد أشرنا إلى أن الإحصاءات تشير إلى أن معظم الحواسيب المحمولة ستصبح مزودة بقدرة الاتصال اللاسلكي. وهذان العاملان يجعلان الحاسب المحمول سلاحاً ذا حدين. و من المتوقع

أن يكون ذلك من الثغرات الأساسية في أنظمة المعلومات، خصوصاً إذا كان جزءا من الشبكة اللاسلكية.

الشبكات المحلية اللاسلكية
Wireless Local Area Networks

اكتسبت الشبكات اللاسلكية – التي تكتب بالإنجليزية اختصارا (WLAN) — وأحيانا يطلق عليها اسم (Wi-Fi) زخما لأسباب أهمها سهولة تركيبها، والمرونة التي تمتاز بها. يضاف إلى ذلك رخص تكاليف إنشائها و صيانتها، و سهولة توسعتها عند الحاجة. وتشير دراسة أعدتها مجموعة (Gartner) البحثية إلى أنه بحلول عام 2006م فإن أكثر من نصف الحاسبات المحمولة ستكون مزودة بالعتاد اللازم للاتصال بالشبكات اللاسلكية[1].

ولكن دلائل الواقع تشير إلى أن نسبة الحاسبات المحمولة المزودة بالعتاد اللازم للاتصال بالشبكات اللاسلكية تفوق بكثير ما ورد في هذه التقديرات الواردة في تلك الدراسة. و مما يؤيد ما ذهبنا إليه أنه ابتداء من عام 2004م أحدث معهد أمن الحاسوب في الولايات المتحدة الأمريكية قسما خاصا بالمشكلات الأمنية للشبكات اللاسلكية في التقرير السنوي الذي يعده مشاركة مع مكتب التحقيقات الفدرالي.

مكونات الشبكة اللاسلكية

إن الشبكة المحلية اللاسلكية هي البساطة ذاتها، فهي تتألف من مكونين ليس غير:

1) بطاقة الاتصال اللاسلكي: تثبت هذه البطاقة في الحاسوب، أو أي جهاز نرغب أن يكون عضوا في الشبكة اللاسلكية، كالطابعات مثلاً. وكما مر معنا فإن معظم الحواسيب المحمولة تأتي مزودة بهذه البطاقة من مصنعها. أما الحواسيب المحمولة غير المزودة بالبطاقة، أو الأجهزة الأخرى فلا بد من تزويدها بها لتكون قادرة على الاتصال. وفي الشكل رقم (56) أحد أنواع كروت الاتصال اللاسلكي الذي يمكن

(1) تقرير بعنوان: "*Swisscom Mobile to launch Public Wireless LAN on December 2002*"

في الموقع: http://www.swisscom.com/media/20020924_EN.html

استخدامه في الحواسيب المحمولة.



الشكل رقم (56): بطاقة الاتصال اللاسلكي.

وينحصر بطاقة في الاتصال تمرير البيانات جيئة و ذهابا بين الحاسوب والشبكة اللاسلكية، فهي نقطة الوصل بين الطرفين.

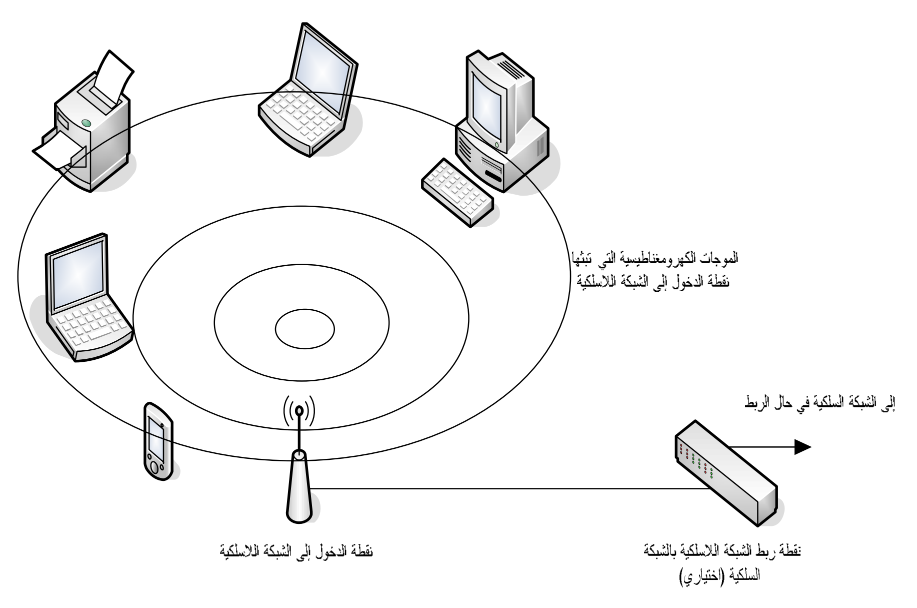
2) نقطة الدخول إلى الشبكة: وهذه تسمى: (Access Point)، وهي جهاز صغير به هوائي صغير، كما في الشكل رقم (57)، ويبث الجهاز الموجات الكهرومغناطيسية لنقل البيانات بين نقطة الدخول و الأجهزة المزودة ببطاقات الاتصال بالشبكة اللاسلكية السابق ذكرها في الفقرة السابقة. وبعمل هذه النقطة مع الأجهزة تتألف لدينا شبكة لاسلكية، كما في الشكل رقم (58).



الشكل رقم (57): أحد الأجهزة التي تستخدم نقطة دخول إلى الشبكة.

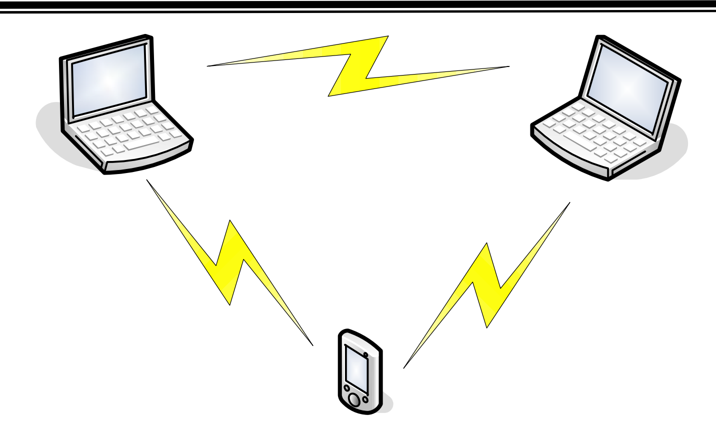
وفي معظم الأحيان نرغب في أن نربط الشبكة اللاسلكية بشبكة المعلومات الأم

في المنشأة، أو بشبكة الإنترنت ؛ ويتحقق هذا بربط نقطة الدخول بالشبكة الأم، أو شبكة الإنترنت، و بهذا يمكن لكل جهاز في الشبكة اللاسلكية الاتصال بالشبكة الأم، أو الدخول إلى شبكة الإنترنت، كما يمكن للمستخدمين في الشبكة الأم، أو شبكة الإنترنت الوصول إلى الأجهزة التي تؤلف الشبكة اللاسلكية.



الشكل رقم (58): شبكة لاسلكية مزودة بنقطة دخول.

كما نستطيع تكوين شبكة لاسلكية دون استخدام نقطة دخول إلى الشبكة، وفي هذه الحال فإن كل ما نحتاجه هو أجهزة مزودة ببطاقات اتصال لاسلكي. ويكون شكل الشبكة كما في الشكل رقم (59).



الشكل رقم (59): شبكة لاسلكية بسيطة (بدون نقطة دخول).

المقاييس المعتبرة في صنع أجهزة الشبكات اللاسلكية

تعود نقطة الانطلاق الحقيقية للشبكات المحلية اللاسلكية إلى العام 1997م الذي شهد ولادة مواصفات (IEEE 802.11) التي تعد أول مواصفات قياسية لهذا النوع من الشبكات. وكأي بداية كانت قدراتها متواضعة من حيث قدرتها على تمرير المعلومات، فلم تتجاوز 2 مليون نبضة في الثانية. كما أنها كانت تعمل في نطاق ترددي قدره 2,4 ميجاهرتز، وهذا يجعلها عرضة للتداخل مع بعض الأجهزة التي تعمل في النطاق نفسه، مثل بعض أجهزة المايكروويف، والهواتف المنزلية النقالة. و لتلافي هذه العيوب توالى صدور المواصفات القياسية. وفي جدول رقم (1) ملخص لأهم خصائص المواصفات الأكثر شيوعاً:

جدول رقم (1). مقارنة لأهم المواصفات القياسية للشبكات اللاسلكية.

اسم المواصفة القياسية	سرعة نقل البيانات	النطاق الترددي الذي تعمل فيه	المزايا	العيوب
IEEE 802.11a	54 مليون نبضة/الثانية	5 جيجا هرتز	• تدعم التطبيقات التي تحتاج وسيلة نقل كبيرة السعة، مثل تطبيقات الوسائط المتعددة كملفات الصوت والصورة • أقل عرضة للتداخل الكهرومغناطيسي من المواصفات الأخرى	• مدى عمل الشبكة قصير، وبالتالي فإن إنشاء الشبكة يحتاج عددا أكبر من نقاط الدخول مقارنة بباقي المواصفات • توفر 8 قنوات فقط داخل الشبكة اللاسلكية[1] • لا تستطيع العمل مع الأجهزة المتوافقة مع المواصفة القياسية IEEE 802.11b

(1) عدد القنوات المتاحة يصبح مهما عندما تنشأ شبكات لاسلكية قد تتداخل موجاتها الكهرومغناطيسية لأننا إذا أردنا إنشاء شبكتين لاسلكيتين و كانتا متقاربتين بحيث يمكن أن تتداخل موجاتهما، فإن علينا أن نتحكم في أوضاع الشبكتين لتعملا في قناتين مختلفتين. بعبارة أخرى فإنه كلما كبر عدد القنوات المسموح بها زادت المرونة المتاحة عند إنشاء الشبكات.

IEEE 802.11b	11 مليـون نبضة/الثانية	2.4 جيجـا هرتز	• مـدى عمـل الشـبكة طويـل، وبالتـالي فـإن إنشـاء الشبكة يحتاج عـددا أصـغر مـن نقـاط الـدخول، مقارنـة بالمواصـفة القياسـية IEEE 802.11a • تـوفر 14 قنـاة داخـل الشـبكة اللاسلكية	• قـدرتها محـدودة علـى تشـغيل التطبيقات التي تحتاج وسـيلة نقـل كـبيرة السعة، مثل تطبيقات الوسـائط المتعـددة، كملفـات الصـوت والصورة • عرضـة للتـداخل الكهرومغناطيسي • لا تستطيع العمـل مع الأجهـزة المتوافقـة مع المواصفة القياسية IEEE 802.11a
IEEE 802.11g	54 مليـون نبضة/الثانية	2.4 جيجـا هرتز	• مـدى عمـل الشـبكة طويـل، وبالتـالي فـإن إنشـاء الشـبكة يحتـاج عـددا أصـغر مـن نقـاط الـدخول مقارنـة بالمواصـفة القياسـية IEEE 802.11a • تـوفر 14 قنـاة داخـل الشـبكة اللاسلكية	• عرضـة للتـداخل الكهرومغناطيسي • لا تستطيع العمـل مع الأجهـزة المتوافقـة مع المواصفة القياسية IEEE 802.11a

وبالنظر إلى مزايا المواصفات التي أدرجناها في الجدول السابق وعيوبها، فإننا ننصح القارئ عند الرغبة في شراء حاسوب بأن يتحرى أن يكون الحاسوب متوافقا مع المواصفات القياسية IEEE 802.11a أو IEEE 802.11g.

كيف تعمل الشبكة اللاسلكية

كما أن مكونات الشبكة المحلية اللاسلكية بسيطة، فكذلك طريقة عملها. وذلك أنه بعد إيصال الطاقة إلى نقطة الدخول إلى الشبكة و الأجهزة المزودة ببطاقة الاتصال اللاسلكي، ووضع الجميع في وضع التشغيل يحدث ما يلي:

3) ترسل نقطة الدخول إلى الشبكة نبضات إلكترونية على فترات منتظمة معلنة عن نفسها.

4) تلتقط الأجهزة هذه النبضات التي تحوي في طياتها معلومات مهمة تساعد الأجهزة على الاستجابة، وتهيئة نفسها للاتصال. ومن أهم هذه المعلومات ما يعرف باسم: (Service Set Identifier)، الذي يعرف اختصارا باسم: (SSID)، وهو ما يميز شبكة لاسلكية عن أخرى.

5) كما تحوي النبضات المشار إليها القناة التي ستعمل عليها الشبكة اللاسلكية.

و لحماية الرسائل المتبادلة داخل الشبكة اللاسلكية تشفر باستخدام نظام تشفير يعرف اختصارا باسم: (WEP)، و لكن نظام التشفير هذا به نقاط ضعف عدة يمكن للمهاجم النفاذ من خلالها، وتهديد الشبكة اللاسلكية.

نقاط ضعف الشبكات اللاسلكية

مر معنا فيما مضى أن للشبكات المحلية اللاسلكية عدداً كبيراً من المزايا، مما يضفي عليها جاذبية يصعب مقاومتها، و لن نجاوز الحقيقة إذا قلنا إن هذه الجاذبية هي وراء كثير من نقاط الضعف الموجودة في هذا النوع من الشبكات، وذلك لأن كثيرين

يندفعون إلى تركيب شبكات لاسلكية، سواء في محيط عملهم أو في منازلهم دون أن يكون لهم أدنى دراية بكيفية عمل الشبكات، والطريقة الصحيحة لتهيئتها، و هذا يقود حتما إلى إنشاء شبكات غير آمنة. و بحسب نسخة عام 2004م من التقرير المشترك الذي يصدره في الولايات المتحدة الأمريكية كل من معهد أمن الحاسوب، ومكتب التحقيقات الفدرالي فإن 15٪ من الجهات التي شملتها الدراسة التي يستند إليها التقرير أفادت بأن شبكاتها اللاسلكية تعرضت لهجمات. كما تشير بعض التقديرات إلى أن مابين 40٪ و 50٪ من الشبكات اللاسلكية إما أن مستوى الحماية فيها ضعيف، أو أنه لا يوجد فيها أي نوع من الحماية على الإطلاق[1].

و مما ينبغي تأكيده أن كثيرا من هذه الهجمات يمكن عملها باستخدام معدات و برامج متوفرة بأسعار في متناول كثير من الناس.

و نقاط ضعف الشبكات اللاسلكية متعددة، يمكن إجمال أهمها في الآتي:

6) بسبب سهولة تركيب الشبكات اللاسلكية وتشغيلها، فإن كثيرا ممن ينصب و يشغل هذه الشبكات هم من الأشخاص الذين ليس لهم درية كافية بأمن المعلومات، و بالتالي فإنهم – في كثير من الأحيان – لا يعرفون كيف يهيئون الإعدادات - خاصة المتعلقة بأمن الشبكة – بشكل صحيح فيتركون ثغرات أمنية كبيرة في الشبكات اللاسلكية التي أقاموها. ومن أمثلة ذلك ترك قيمة (SSID) الأصلية دون تغيير، مما يسهل على المهاجم الاشتراك في الشبكة اللاسلكية. و إذا كانت المنشأة لا تملك سياسات تحدد ما يمكن عمله وما لا يمكن فيما يتعلق بأمن المعلومات، فإنه كثيراً ما يقوم الموظفون بتركيب شبكات لاسلكية دون علم الجهة المسؤولة عن تقنية و أمن المعلومات. و يكون الأمر أشد خطرا إذا كانت الشبكة اللاسلكية مربوطة بالشبكة الأم

---

(1) Informit.com, March 2005

للمنشأة، لأن ذلك يعني فتح ثغرة خفية في الدفاعات التي أقامتها الجهة المسؤولة عن تقنية و أمن المعلومات.

7) وضع نقاط الدخول إلى الشبكة في أماكن مفتوحة مثل الممرات، والقاعات، أي أنه بإمكان أي شخص أخذها من موقعها و العبث بإعداداتها، ما يسهل عليه شن الهجمات، ثم إعادتها في مكانها الأصلي.

8) سهولة تعرضها للهجمات المؤدية إلى تعطيل الخدمة (Denial of Service) الذي يجعل أعضاء الشبكة اللاسلكية غير قادرين على تبادل المعلومات بينهم. هذا النوع من الهجمات يعد من أخطر ما تتعرض له الشبكات اللاسلكية لاعتبارات أهمها:

أ) إن الشبكات اللاسلكية تعتمد على نطاق ترددي ضمن الطيف الكهرومغناطيسي لنقل البيانات، و يمكن بسهولة التشويش على ذلك النطاق الترددي لتوفر الأجهزة اللازمة للتشويش ورخص ثمنها.

ب) وفقا لما جاء في نسخة عام 2004م من التقرير المشترك الذي يصدره في الولايات المتحدة الأمريكية كل من معهد أمن الحاسوب و مكتب التحقيقات الفدرالي، فإن هجمات تعطيل الخدمة تبوأت المركز الأول – مشاركة مع الهجمات باستخدام البرامج السيئة – من حيث حجم الأضرار الذي تنزله، و هذا يدل على أن عددا كبيرا من المهاجمين صاروا يعتمدون هذا النوع من الهجمات.

ج) هناك ثغرات في تصميم البروتوكول الذي يدير عملية انضمام الأعضاء إلى الشبكة، وقد مر معنا أنه أثناء تأسيس الاتصال بين نقطة الدخول و الأجهزة الراغبة في الاتصال بالشبكة ترسل نقطة الدخول نبضات إلكترونية على فترات منتظمة معلنة عن نفسها، وأن هذه النبضات تحوي في طياتها معلومات مهمة تساعد الأجهزة على

الاستجابة، وتهيئة نفسها للاتصال. وتستمر نقطة الدخول إلى الشبكة في إرسال هذه النبضات طيلة فترة عملها للمحافظة على الاتصال بين أعضاء الشبكة. ولكن المشكلة أن الرسائل التي تحملها هذه النبضات تبث دون أي نوع من الحماية، فليس هناك ما يدل - بشكل قطعي- على هوية من أرسلها، و بالتالي فإنه يمكن للمهاجم إرسال نبضات مزورة تحمل هوية نقطة الدخول الحقيقة، و يحمل تلك النبضات رسالة تطلب من جميع الأجهزة المرتبطة بالشبكة إنهاء الاتصال، و هذا يقطع عمل الشبكة و يعطل الخدمة.

9) أيضاً بسبب طريقة عمل الشبكات اللاسلكية و اعتمادها على الطيف الكهرومغناطيسي، فإنها عرضة للتنصت بشكل خطير، نظراً لوجود أجهزة خاصة يمكن للمهاجم استخدامها لبث نداءات لاسلكية. وبسبب طبيعة عملها فإن نقطة الدخول إلى الشبكة تستجيب لهذه النداءات، مما يكشف وجود الشبكة اللاسلكية، وعندها يقوم المهاجم باستخدام أجهزة أخرى لالتقاط الرسائل المتبادلة داخل تلك الشبكة. و قد مر بنا أن الرسائل المتبادلة يمكن حمايتها باستخدام نظام تشفير (WEP)، و كما ذكرنا سابقاً، فإن هناك نقاط ضعف في نظام التشفير هذا، منها قدرة المهاجم على معرفة المفتاح المستخدم في عملية التشفير، و بالتالي يمكنه فك تشفير الرسائل التي التقطها.

وسائل حماية الشبكات اللاسلكية

تتطلب حماية الشبكات اللاسلكية اتخاذ عدد من الخطوات الاحترازية، يمكن إجمال أهمها في النقاط التالية:

1) وضع سياسات تحدد المسموح به، والممنوع فيما يتعلق بأمن المعلومات، و توفير آليات لتنفيذ تلك السياسات، واكتشاف المخالفين و التعامل معهم.

2) التحقق من أن الشبكات اللاسلكية تنشأ و تدار من قبل أشخاص

متخصصين في هذا المجال، ومنع الهواة، وقليلي الدراية من القيام بهذه الأعمال. كما يجب التأكد من أن كل ذلك يتم وفق سياسات وإجراءات تضمن أمن المعلومات.

3) تغيير الأوضاع الأصلية لمعدات الشبكات اللاسلكية وبرامجها، وهذا يجب أن يكون نتيجة حتمية للخطوات السابقة.

4) مراقبة شبكات المعلومات لاكتشاف أي أنشطة مشبوهة.

5) حسن اختيار المواقع التي توضع فيها نقطة الاتصال بالشبكة بحيث تكون النقطة محمية، كما يكون بثها الكهرومغناطيسي موجها إلى داخل البيت، أو المنشأة قدر الإمكان، وتقليل ما يبث نحو الخارج لتقليل فرص التقاط البث.

6) تشغيل بروتوكولات التحقق من الهوية و أنظمة تشفير قوية لتأمين المعلومات.

الخلاصة

لشبكة الاتصال اللاسلكي مميزات كثيرة لا يمكن إنكارها، ويندر أن توجد منشأة ليس فيها شبكة لاسلكية. و الذي يجب التنبه إليه هو أنه بسبب الثغرات الكثيرة في الشبكات اللاسلكية، وما قد ينجم عن ذلك من اختراقات لأنظمة المعلومات فإن على الشركات و المنظمات السيطرة على الشبكات اللاسلكية- إنشاء وتشغيلا- ؛ كما أن عليها وضع السياسات و الإجراءات التي تكفل ذلك.

معجم مفردات أمن المعلومات

Adware	برامج الإعلانات
Attachments	مرفقات
Attacker	المهاجم
Authentication tools	وسائل التحقق من الهوية
Automatic Updates	التحديث التلقائي / الآلي
Availability	ضــمان الوصـــول إلى المعلومــات والمــوارد الحاسوبية / الوجود
Backdoors	أبواب خلفية
Biometrics	المقاييس الحيوية
BIOS	النظام الأساس
Black List	القائمة السوداء
Browser	البرنامج المتصفح
Brute Force	الطريقة الاستقصائية
CD	القرص المدمج
Computer	حاسوب
Configuration	تهيئة
Cookies	الكعك أو ملفات تعريف الارتباط
Crack	تصديع
Critical Updates	التحديثات الحرجة
Data Confidentiality	سرية المعلومات
Data Integrity	سلامة (أو تكامل) المعلومات

Decrypt	يفك التشفير
Default Configuration	أوضاع التهيئة الأصلية
Denial of Service	تعطيل الخدمة
Dialog Box	صندوق حواري
Discoverable	وضع قابل للاكتشاف
Docking Station	محطة تثبيت
Domain Name	اسم النطاق
Download	تحميل
Eavesdropping	التنصت
E-mail	البريد الإلكتروني
E-mail account	صندوق البريد الإلكتروني
E-mail address	عنوان إلكتروني
E-mail Best Practices	أفضل طرق التعامل
E-mail client	برنامج البريد العميل
E-mail Filtering	فرز البريد الإلكتروني
E-mail Server	خادم البريد الإلكتروني
Encrypt	يشفر
Engineering	الهندسة الاجتماعية
Filtering	غربلة
Firewall	جدار حماية
Hackers	قراصنة الإنترنت/ المتطفلون

Help Desk	مراكز تقديم الدعم الفني
Heuristics Engines	محركات القواعد المساعدة
Hoax	الخداع أو البلاغ الكاذب
Hotfixes	التعديلات السريعة
Inquiry	استفسار
Install	تنصيب
Installation	تنصيب
Instant Messenger	المراسل الآني
Intruder	المهاجم
IP Address	العنوان الرقمي المميز للحاسوب
Junk mail	البريد غير المرغوب فيه
Keystroke Logger	برنامج تسجيل نقرات لوحة المفاتيح
Laptops	الحواسيب المحمولة
Malicious codes	البرامج الخبيثة
Malware	البرامج الخبيثة
Master	المتبوع
Message body	فحوى الرسالة
Model	طراز
Network Address Translation	تحويل العناوين الرقمية
Non-Discoverable	وضع غير قابل للاكتشاف
Packet Filtering	غربلة مظاريف البيانات المرسلة

Packets	مظاريف إلكترونية
Pairing	تأسيس الارتباط
Password	كلمة المرور
Personal Digital Assistant	المساعد الرقمي الشخصي
Phishing	رسائل الاصطياد الخادعة
Physical Security	الحماية المادية
Popup	الصفحات الفقّاعية أو الانبثاقية
Port Social	نقطة عبور
Product ID	الرقم المميز للمنتج
Product Key	المفتاح الخاص بالمنتج
Proxy	وكيل
Region and Language Setting	أوضاع المنطقة واللغات المحملة
Reversed Social Engineering	الهندسة الاجتماعية العكسية
Router	موجه
Scam	عمل خدّاع
Screen Savers	شاشات توقف
Script Kiddies	أطفال البرامج الجاهزة
Security Updates	التحديثات الأمنية
Server	الخادم
Service Pack	الرزم الخدمية
Slave	التابع

Smart Cards	البطاقات الذكية
Software Fix	بريمج علاجي
Spyware	برنامج متابعة تصرفات المستخدم أو التجسس البسيط
Standardization	تنميط
Stateful Inspection	مراقبة السياق
Subject	موضوع الرسالة
Switch	المقسم
Synchronization Software	بريد التناغم
Target user	المستهدف
Tools	الأدوات المساعدة
Upgrade	إصدارات الترقية
User name	اسم المستخدم
Version number	رقم النسخة
Virus	فيروس
Vulnerability	ثغرة
White List	القائمة البيضاء
Windows GUID	رقم التعريف العام لنظام ويندوز
Wipe	طمس
Worm	دودة
www	الشبكة العنكبوتية العالمية

فهرس الموضوعات

فهرس الأشكال

ماذا قالوا عن الكتاب

إن هذا الكتاب (أمن المعلومات بلغة ميسرة) يقدم وسيلة بالغة القيمة والفائدة لتوعية و تعليم المتخصص و غير المتخصص بأهم مبادئ و أساسيات و وسائل الوقاية من أخطار أمن المعلومات. كما أن أسلوبه الكتابي شيق و سلس ويوحي بالجهد الكبير الذي بذله المؤلفان و يجعله من خير ما ألف في هذا المجال بالغة العربية.

د. محمد بن عبدالعزيز العقيلي

مدير عام تقنية المعلومات

هيئة الدواء والغذاء

*****

قدم تغطية شاملة وبلغة مبسطة لجوانب عديدة في مجال أمن المعلومات، وهي غالبية ما يحتاجه المستخدم العادي غير المتخصص في المجال، ويعتبر من أفضل الكتب التي سبق لي الإطلاع عليها في هذا الجانب حتى باللغة الانجليزية. وأعتقد بأنه ومع الطفرة الحالية في مجال تقنية المعلومات والاتصالات في المملكة، فإن هذا الكتاب قد تم تقديمه في الوقت المناسب ليسد بعض الثغرات الموجودة لدى المستخدمين وجهد تشكرواً عليه.

عمر بن عبد الله النعماني

مدير عام أمن المعلومات

شركة الاتصالات السعودية

*****

إن هذا الكتاب قد يكون من أشمل ما كتب عن مبادئ أمن المعلومات، وقد بذل مؤلفيه جهداً مشكوراً في توضيح وتبسيط الكثير من المصطلحات والمفاهيم الأساسية الخاصة بأمن المعلومات، ويعد مرجعاً مفيداً في مجال أمن المعلومات.

صقر العرابي الحارثي

مدير أمن المعلومات

مؤسسة النقد العربي السعودي

*****

إن هذا الكتاب سيدخلك إلى عالم أمن المعلومات بلغة سهلة وميسرة دون الخوض في كثير من التفاصيل، وكذلك يعطيك طرق سهلة للوقاية من الأخطار التي تهدد أمن المعلومات. لذا فأنا أعتبره مثالي لأي شخص يريد فهم عالم أمن المعلومات.

علي إبراهيم المزيني

مدير أمن المعلومات ببنك البلاد

*****